CANADIAN CYBERSECURITY 2018

An Anthology of CIO/CISO Enterprise-Level Perspectives

AMIR BELKHELLADI
Partner, Risk Advisory Leader - Eastern Canada, Deloitte

DOLEV FARHI
Lead Security Engineer, Paytm Labs / Founder, DEFCON 416

EDWARD KILEDJIAN
VP Information Security, Compliance and CISO, OpenText

JEFF STARK
VP, Technology Risk and CISO, IGM Financial

MIKE REDEKER
VP and CIO, Canadian Pacific Railway

ROBERT W. (BOB) GORDON
Executive Director, CCTX

SHEILA JORDAN
CIO, Symantec Corp.

VIVEK KHINDRIA
Head of Cyber and Information Security, Bell Canada

Edited by **AJAY K. SOOD** *VP, Country Manager,* Symantec Canada

CLX FORUM
Enabled by Symantec

CANADIAN CYBERSECURITY 2018

An Anthology of CIO/CISO Enterprise-Level Perspectives

CANADIAN CYBERSECURITY 2018
An Anthology of CIO/CISO Enterprise-Level Perspectives

ISBN 978-1-5445-1193-1 *Hardcover*
978-1-5445-1192-4 *Paperback*
978-1-5445-1191-7 *Ebook*

CONTENTS

ACKNOWLEDGMENTS

I owe a special thanks to everyone who contributed to this book, both on the written pages and behind the scenes.

Steve Tso, you are a superstar and you made it happen. Thank you for your countless hours devoted to this project. I also want to thank my entire team at Symantec. Your hard work behind the scenes helped this project take flight and stay in the air.

Deep gratitude to all of our contributors: Amir Belkhelladi, Bob Gordon, Dolev Farhi, Edward Kiledjian, Jeff Stark, Mike Redeker, Sheila Jordan, and Vivek Khindria. You all impressed me with your deep knowledge and expertise. Thank you for sharing your wisdom in these pages. I am eternally grateful.

And finally, to my daughters, Diya and Anya, for continuing to inspire me to be better every day and for reminding me why I want to help make your world safer.

INTRODUCTION

AJAY K. SOOD, VP, COUNTRY MANAGER, SYMANTEC CANADA

With over twenty years of real-life, in-the-trenches business experience in the IT security space, Ajay is a seasoned veteran in introducing disruptive security brands to the Canadian market. He currently serves as the VP of Symantec Canada, where he is on a mission to help organizations stay ahead of the curve in architecting and operating their cybersecurity defences. You can follow him on Twitter @akssecure.

Would you prefer to take the red pill or the blue pill?

That question is a reference to the popular science fiction action movie *The Matrix*. In the film, Neo rebels against tyrannical machines that keep humans enslaved in a simulated reality. According to Wikipedia, "The red pill and its opposite, the blue pill, are a popular cultural meme, a metaphor representing the choice between knowledge, freedom, and the brutal truths of reality (red pill), and security, happiness and the blissful ignorance of illusion (blue pill)."[1]

1 Wikipedia, "Red pill and blue pill," last edited July 24, 2018, https://en.wikipedia.org/wiki/Red_pill_and_blue_pill

In the world of cybersecurity, blissful ignorance and a false sense of security (the blue pill) will undoubtedly end in disaster. This book is the red pill. It will expose the brutal truth and harsh reality of the cyber threat landscape facing organizations today and then suggest the necessary knowledge and analyze appropriate solutions and strategies for combatting those threats.

FOLLOW THE DATA

The world is changing, and cybersecurity threats and defences are changing along with it. Organizations today collect and store more data than ever, in more places than ever, which has created a follow-the-data problem. Data must be created, collected, stored, controlled, and destroyed securely, and the human and financial costs of following this data are greater than they've ever been. There is a need to help organizations understand and address this challenge, and this book meets that need.

The book is neither a beginner's guide nor an introduction to cybersecurity. If you're looking for that type of a resource, there are plenty out there. Rather, the purpose of this book is to bring together eminent thought leaders and top cyber professionals in the Canadian information security industry to discuss current issues and trends from a leadership perspective.

What makes this book special, and targeted, is its strict focus on Canadian cybersecurity. There is a lot of material out there for a global audience, a European audience, a United States audience, and an Asian audience, but there is precious little tailored specifically to the Canadian market. My hope and my goal in putting this publication together is to give Canadian readers information and actionable advice that is directly relevant to Canadian cybersecurity practitioners.

CANADA IS UNIQUE

Canada is a unique and special country, especially in regard to cyber. Canada's economic prosperity is closely tied to its largest trading partner, the United States. Therefore, Canadian firms tend to have the lofty ambitions of Americans. Canadian startups, incubators, and enterprise companies all dream of being the next global blockbuster success. Plus, Americans populate the executive landscape in companies all over Canada. In many of the largest Canadian organizations today, you don't have to look very far before you see an American running the cybersecurity show as chief information security officer (CISO), chief information officer (CIO), or any other relevant technology executive.

Although Canadian firms aspire to make it big like their American counterparts, Canada has a regulatory climate

more in line with the European Union. Canadians tend to value personal privacy and demand protection of personal information more than Americans. There is no current universal American equivalent to Europe's General Data Protection Regulation (GDPR) or Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) or Digital Privacy Act (DPA).

Now combine those two elements—big dreams and Euro-style data regulations—with the fact that Canada has the budgetary constraints of Latin America. As such, cybersecurity expenditures are limited. On the other hand, one of the cool things about having a micro-economy is that it's easier to steer. These points, in my opinion, are what make Canada unique in both international business and in the global cybersecurity landscape.

CANADA RISING

There are plenty of Canadian success stories. Elon Musk went to school at Queen's University in Ontario, and he's one of the world's great innovators. The Kitchener-Waterloo region is the Silicon Valley of the North, and home to cutting-edge technology research schools like the University of Waterloo, which is widely regarded as a leading technology school in Canada. Major tech players like Microsoft, Google, and Facebook routinely recruit students from this area.

Kitchener-Waterloo is also the birthplace of BlackBerry/Research in Motion (RIM), OpenText, and CacheFlow, which grew into Blue Coat, which in turn merged with Symantec, the company I work for now. Nova Scotia and New Brunswick are also emerging hotbeds of entrepreneurship and startup incubators, with their governments bolstering innovation and investment in cybersecurity. These are examples of Canadian success stories.

Many schools in Canada now offer dedicated diplomas and certifications in cybersecurity. Students can enter two-, three-, or four-year programs in cybersecurity and graduate with useful and marketable skills. These programs have broadened the cyber talent pool from which big companies can recruit. In fact, some college kids are graduating at age twenty-one or twenty-two with degrees in cyber and fielding multiple job offers. That type of opportunity just didn't exist a decade ago. Yet, there is still a massive skills shortage in cyber, a problem you'll read about in Chapter 4.

Canada has a track record of innovation, a proven and growing talent pool, and a culture of technological entrepreneurship. It's one of the most wired and networked countries in the world. In fact, a higher percentage of homes in Canada have access to high-speed internet than in the United States, and Canada is fostering a cyber boom modelled after the tech boom in Israel. It is my sense that

Canada is on the cusp of a Cyber-Renaissance. Many of the contributors you'll meet in the following chapters are pioneers leading the way.

CYBERSECURITY IS NEEDED EVERYWHERE

Cybersecurity has expanded to the point of being all-encompassing. Technology is a part of everything we do. We live on our devices, and we all share in the cloud. From mobile banking to dating apps to daycare monitoring, we put all aspects of our lives online. If it's online, it's vulnerable to attack. When it comes to business, cyber is an essential enabler for enterprises in Canada and around the world. But if you can't protect your data, you won't remain in business. It's that simple.

Every technology—from Snapchat to autonomous cars to space travel—must have cybersecurity built in. In the past, I would have said you need to wrap your technology in security. But now, more than ever, security must be built into the technology, baked in the cake—or even better, mixed into the dough—instead of creating just a wall to keep the bad guys out. Security is an essential component of every critical system; it's no longer a separate protective layer that can be added later. Security, therefore, is a critical element of any organization's operating plan.

EVOLUTIONS IN CYBERSECURITY

As I mentioned at the top of this introduction, the world is changing. Cybersecurity strategies and processes must adapt with this change. In the past decade, we've seen a dramatic evolution in the cybersecurity world in four key areas: cyber capitalization, types of cyberattacks, countermeasures employed, and regulatory climate. It's important to review this evolution so you can understand where the cybersecurity industry has been, where it is right now, and where it's headed. This understanding will hopefully guide your decisions going forward.

CYBER CAPITALIZATION

Cyber capitalization refers to how attackers, or hackers, intend to capitalize on a cyberattack. The first wave of capitalized attacks generally focused on financial gains. Hackers attempted to steal credit card information, access bank accounts, or otherwise rob financial valuables from their victims. This evolved into intellectual property theft, where hackers would steal proprietary technology, patents, trade secrets, or other valuable information. The next big wave in cyber capitalization saw nation states, governments, or political organizations illegally accessing or stealing classified or confidential documents about government activities and policies, or crippling critical infrastructure.

The latest evolution in cyber capitalization is the theft or destruction of personal capital. This is when hackers steal private information on a person, such as their address, children's names and school, what prescription drugs they take, their religion, political affiliations, charitable donations, race or ethnicity, even sexual preference. It is this phase that has spawned new government regulations and made cybersecurity more relevant to individuals than it has ever been before. No one wants that type of deeply personal information leaked or sold to the highest bidder on the dark web.

TYPES OF CYBERATTACKS

We also have seen an evolution in the sophistication of cyberattacks that hackers employ to get what they want. In the beginning, hackers attacked infrastructure and hardware. This included distributed denial of service (DDoS) attacks, brute force attacks on routers or other pieces of equipment, and simpler protocol-based attacks on firewalls.

From attacks on infrastructure rose more sophisticated attacks on data. Attackers didn't care about the infrastructure anymore because they found something way more valuable: important data. Malware, botnets, and targeted attacks began to flourish and evolved into direct attacks on individuals. These attacks include identify theft,

spear phishing, and other methods of stealing private, personal information.

COUNTERMEASURES

As the types of attacks evolved over time, so too did the countermeasures organizations employed to combat those attacks. Initially, many of these countermeasures were tools-based defences, like firewalls and antivirus software. As the complexity of attacks increased, these tools needed to be supplemented with human-based defences, which saw the advent of security operations centres and human monitoring of systems.

Clearly, as the adversary became more human, so too did the countermeasure—but that didn't address the scale of the problem. Information overload became rampant, and the value of intelligence rose. Investigations, digital forensics, and chain of custody became essential, though very effort intensive. Analytics and advanced data processing soon became essential for triage.

The latest evolution in both the type of attacks and countermeasures involves using artificial intelligence (AI). The number of artificial-intelligence-based attacks is on the rise. Attackers are now using AI to launch smart attacks to probe cyber defences for any weakness or vulnerability. To combat AI-based attacks, organizations

must employ AI-based defences, which are costly and still in their infancy.

REGULATORY CLIMATE

The fourth evolution we've seen in cyber is in the regulatory environment. The first wave of regulation began after a number of widely publicized data breaches at major organizations. This led to a round of lawsuits demanding damages for those consumers whose information was compromised. Next, government legislative bodies passed laws to regulate how organizations collect, store, and use private data. The most far-reaching regulation to date is now in effect in Europe under the GDPR, which will be discussed in greater detail in Chapter 12.

The aforementioned evolutionary trends demonstrate how cybersecurity has grown as a field of study in size and complexity. As the adversary changes its tactics and targets, organizations must alter their defences and countermeasures. Any organization that falls behind the current state of the art in cyber does so at its own peril.

THE CONTRIBUTORS

You've heard the phrase "Diversity is our strength." We believe in that ethos. When we decided to create this book, we naturally wanted a diverse group of voices and

perspectives. We selected eight of the top thinkers in security and asked them to write about what they know best. These contributors represent a relevant cross-section of the debates and discussions going on now in the cyber industry. We have corporate leaders, software gurus, representatives from government, even the CIO of the largest cybersecurity company on the planet. If our goal was to put together a cybersecurity dream team, then mission accomplished.

In truth, any one of us could have written this book on our own and done an admirable job. But that would result in a book from one person's viewpoint, from one perspective. In contrast, having eight different contributors—each with their own unique perspective—is what makes this book enormously valuable. Our contributors represent a cross-section of Canadian cybersecurity expertise and thought leadership you won't find in one place anywhere else.

As for how we chose the topics in the book, we were deliberate and thoughtful. We didn't just search the web for a list of current topics in cybersecurity. We thought deeply about which issues would be most pertinent to Canadian organizations currently and in the future. The list started with twenty-five topics. After much discussion and debate, we whittled it down to the twelve most crucial and relevant topics to Canadian cyber professionals.

In Chapter 1, Sheila Jordan covers security as a service. In Chapter 2, Jeff Stark discusses how to build a defensible, self-defending network. In Chapter 3, Amir Belkhelladi guides the reader in how to coach a board of directors and company leadership on cybersecurity issues. Chapter 4, by Edward Kiledjian, covers the cybersecurity talent shortage. Chapter 5, about information sharing and collaboration, is by Bob Gordon. "Moving from Waterfall to DevOps Frameworks" is Vivek Khindria's topic in Chapter 6. The title of Chapter 7, by Dolev Farhi, is "You Can't Protect the Unknown: Establishing and Maintaining Visibility." Chapter 8, also by Dolev, is about protecting global brands and reputations. Mike Redeker wrote Chapter 9, about managing multiple vendors and vendor churn, and also Chapter 10, about managing big data effectively. Chapter 11, another by Amir Belkhelladi, examines which security considerations to put forth and how to do it. Finally, in Chapter 12, we take a deep dive into GDPR with Edward Kiledjian.

How's that for a lineup?

One of the biggest paradigm shifts in cybersecurity is the explosion of cloud computing. This massive migration of data to the cloud makes sense from a financial and operations standpoint. But from a cybersecurity standpoint, storing data in the cloud is fraught with peril. So that's a great place to begin. Please turn the page to read what Sheila Jordan has to say about security as a service.

CHAPTER 1

SECURITY AS A SERVICE

SHEILA JORDAN: CIO, SYMANTEC CORP.

Sheila Jordan is chief information officer at Symantec Corp., the world's largest cybersecurity company. She is responsible for driving Symantec's information technology strategy and operations, ensuring that the company has the right talent, stays ahead of technology trends, and maximizes the value of technology investments. Since joining Symantec in February 2014, Sheila has set the vision and strategy for Symantec IT, developed an experienced leadership team, and insourced IT operations from an outside vendor, building Symantec's next-generation secure data centre in the company's virtual private cloud. Sheila led the effort to split IT operations when Symantec separated its security and information management businesses through the divestiture of Veritas—a highly successful, transformative initiative accomplished in nine months. Prior to joining Symantec, Sheila served as senior vice president of communication and collaboration IT at Cisco Systems and senior vice president of Destination Disney. She holds a Bachelor of Arts degree in accounting from the University of Central Florida and an MBA from the Florida Institute of Technology.

Security as a service is an undeniable necessity at this point in the evolution of cybercrime and the challenge of modern cyber threat mitigation. The sophistication of the adversary

and the complexity of attacks have increased to such a degree that organizations today are not staffed for the level of threat they face.

Most organizations can combat the commodity attacker or the automated attack. However, when facing advanced persistent threats (APT) and nation-state-class attacks, more powerful defensive tools are needed. It's almost an unavoidable necessity to partner with a security-as-a-service provider or another external entity to augment your security team. This needs to be done thoughtfully and with intent prior to any security event. It should be a part of any organization that's serious about their security program. —Ajay K. Sood

The rapidly changing world of cybersecurity is one of the most critical and exciting areas of technology. This world forces new demands on executives, requiring them to demonstrate business acumen and creativity. Here's where CIOs are uniquely suited to make an impact—not just on security but also on the growth and evolution of the organizations they help protect. It starts by developing the right strategic framework and understanding how to leverage the latest technologies; it results in the reinvention of business processes and the pursuit of innovation at every turn.

STRATEGICALLY OPERATE, EVOLVE, AND GROW A COMPANY WITH IT AND TECHNOLOGY INVESTMENTS

As a CIO, I divide my responsibilities into three categories. First on that list: what resources are required to run the organization at a base level? I then need to figure out how to optimize those resources so that any enhancements foster positive changes. Ultimately, I regularly review how our technology investment is contributing to revenue growth.

Every CIO faces the same challenge balancing supply and demand. Simply put, there is always more to do than there are resources and funds available. Unfortunately, IT is often viewed within the organization as the easiest place to cut costs. While that conjures up a Mission Impossible scenario, remember that a big part of our job is to continue optimizing costs in the most effective way possible for the organization. In practice, that means we must prioritize the demands that most directly affect the profitability and financial goals of the company.

Most CEOs have historically thought of IT only as an operational function. Obviously, the entire company benefits when IT helps things run smoothly. But that's no longer enough.

IT and technology investment now are as much of a strategic lever as the investments organizations make in other

divisions, such as marketing or sales. They increasingly affect how the business interacts with the outside world as well as with its employees. Indeed, there's now the expectation that our investments in technology should impact and satisfy all our stakeholders—employees, partners, and customers—as we help quarterback the process of digital transformation inside our companies.

Consider, for example, the ways in which consumers regularly interact with companies. You can buy everything from a bottle of Windex to a generator in less than three clicks using your phone or personal computer. Besides raising new customer expectations about ease of use, the consumerization of IT also means that CIOs must approach change in a different way.

It's our job to help manage the process of technological transformation. That means paying attention to make sure that every investment dollar counts. Whatever we save, we can later reallocate to other areas. Certainly, you'll find no shortage of areas that need enhancements. But nobody has an unlimited budget, so be prepared to prioritize your technology investments to derive optimal value. You need to develop a business plan with specific attention to ROI and other key metrics. That will provide an invaluable set of talking points when the company decides what it will need to fund to help drive new growth.

FIVE TRENDS

Despite so much technological change, the role of the CIO has not fundamentally changed over the years. We are still responsible for protecting the company's largest asset: the data belonging to its employees, customers, and partners. At the same time, we're still on the hook for helping the company derive actionable insights from that information. What has changed over the years is how CIOs go about their work. Five years ago, we managed our own physical data centres and ran monolithic applications. Sometimes, you found installations running only desktop PCs (this was back in the digital Stone Age, before the world moved to laptops and mobile devices). If you think about the company as a house with four walls, we were essentially managing everything within a four-walled structure where we had total control and complete visibility. What's more, data rarely ventured beyond the perimeter.

That's all in the rear-view mirror. We're living through a period of unparalleled digital change taking place at a rapid-fire clip. The embrace of mobile, the growth of the Internet of Things (IOT), the transition to cloud applications, including software as a service (SaaS) applications and infrastructure as a service (IaaS)—the net effect has been to transform the way that we do everything. It is simultaneously exciting and challenging. And it has also created myriad new expectations among employees, partners, and customers. The new norm in business: Make it fast, make it

simple, and make it relevant. And while you're at it, make sure to turn this into a "know me" experience as well.

For CIOs, there are more variables than ever to manage, ranging from security to access and identity. So, when we consider the CIO's role in protecting company data and making it useful, we must take note of the fact that data is now more fluid than ever. You find it both inside and outside of the firewall, zipping between mobile devices and remote data centres. Let's step back to consider five technology trends that spotlight how the fast pace of change in IT has impacted the CIO's job:

1. The mass move to mobile. Last year, there were four and a half billion phones worldwide; that number increases to eight billion when you add the other mobile-connected devices. The market's hardly done growing, and you can expect that number to climb to nine billion in 2020.
2. Software as a service is the new norm. Most applications today are SaaS, which comprises approximately 65 percent of the applications across the entire IT landscape.
3. IaaS is transforming how we think about cloud computing, data centres, labs, and infrastructure services.
4. Unstructured data is merging with structured data to inform near real-time decision-making. For years, companies ran their businesses using structured data.

But thanks to the plethora of social data, we now can help companies make better use of the wisdom of the crowd. For example, a company nowadays can launch a social campaign and know within minutes whether it is going to work.

5. A veritable explosion in the number of IoT devices is underway. Some estimates project as many as thirty-five billion connected devices will exist within two years. That could present managerial challenges if employees connect their own IoT devices—including family photos, health records, and other personal data—to the corporate network.

HOW THE TRENDS AFFECT EMPLOYEES AND CUSTOMERS

As these five technology trends play out, they raise exciting possibilities for employees to work more efficiently, and for customers, who benefit from faster communications and updates. Think about how technology now delivers "mobile moments of productivity" that allow us to get so much more accomplished. People now constantly multi-task, answering emails and text messages in real time. You can be on a beach or in line at the bank and find people finishing work-related tasks between meetings.

Historically, employees spent much of their time on workstations and desktops. All the technology was corporate-owned and there was a distinct separation

between devices used for work and home. Most of those barriers have since fallen away, and the separation between work and home technology has blurred. When it comes to technology, employees nowadays also happen to be sophisticated consumers. As more IoT devices enter the market—everything from medical devices to drones—the expectations around *employee experience* will continue to be revised and redefined.

The expectations around *customer journey* are also increasing. People can use any number of apps on their phones to buy products and services from companies. The digital age has taught them to be impatient, and they expect companies they interact with to provide relevant information and let them buy what they want within a few clicks. For repeat purchases, they should be able to process the order in even fewer clicks. These expectations revolve around simplicity and sophistication. Think of rideshare services, such as Uber and Lyft, where a customer engages entirely through their phone to receive the service. It's the ultimate example of what it means to live in a frictionless economy: they never need to talk to another person.

USING ADVANCEMENTS IN TECHNOLOGY TO CHANGE AND GROW THE ORGANIZATION

All these sundry advancements in technology offer CIOs an incredible opportunity to help their companies change

and grow. One of the primary ways is through the deployment of SaaS. At Symantec, for example, 65 percent of the applications we use are based on SaaS—everything from Box to WebEx to Eloqua to Zuora.

Elsewhere, IaaS and public cloud provide further opportunities for change. At Symantec, most of our consumer business runs on the Azure public cloud, while we rely on AWS for many of our cloud products and services in both consumer and enterprise.

These three levers—SaaS, IaaS, and cloud—have let us simplify our environment and become more agile in the way that we work and deliver services to employees, customers, and partners.

SIMPLICITY AND AGILITY WITH SAAS

The benefits of using SaaS applications are many. In the past, an upgrade to a large application could take six to nine months. IT would have to take the application down and get another version up and running. If the organization used a legacy application, the process would be even harder, requiring a major jump past several versions. The whole technology stack would need to be evaluated. How was the application optimized? How was it working with the databases? How was it working with the existing infrastructure?

When a SaaS provider upgrades and patches on a regular basis, almost in real time, you don't have to take an application out of service. The software providers do all the back-end work for you. Version control becomes less important. Enhancements come through automatically. It's like the way that little red badge icon in Settings on your iPhone works. It allows you to upgrade your operating system in one click. You don't see the complexities behind the scenes. It's the same with getting the upgrades from all the apps you use on your phone. In minutes, you can upgrade all your applications. That is incredibly powerful for agility and keeping relevant.

When you apply that concept at an enterprise level and applications are being updated and upgraded automatically, you gain a huge advantage. Organizations no longer must take away critical resources from IT or make an upgrade to handle a huge project or event. With SaaS, I no longer need to dedicate as many people as before to do that work. We certainly need to always understand the upstream and downstream effects that a SaaS application will have on data and other applications. Still, this frees people up, so they can instead focus on driving innovation and new capabilities. That's essential if the IT team is going to be able to drive business value.

The ultimate payoff is that you and your employees will benefit from the upgrades, which provide greater sta-

bility, productivity, and capabilities. Meanwhile, IT can help make the SaaS application more relevant and more personalized by evaluating that data horizontally across applications. At Symantec, we delivered a global subscription platform that links our core engineering platform with Zuora, SFDC, and Oracle for billing and financials. Thanks to our increasing move to cloud products, there's more demand for subscriptions. We can allow our customers and partners to trial our products and services. If they want to buy them, they can wrap up the purchase in a few clicks. Their purchase runs through a set of processes and systems that make it seamless to outsiders. This goes back to my earlier point regarding the consumerization of IT and what that bodes for the customer experience. No one wants to go through an ERP workflow to order an endpoint protection product for a small business, wait for a purchase order, and then download it hours later. It needs to happen at consumer speed.

Just as Symantec consolidated our applications using SaaS, we decided to consolidate our data by migrating to public cloud eighteen months ago. With our eight acquisitions and two divestitures, we had an opportunity to streamline and simplify our entire infrastructure, including global data centres and labs. When we acquired LifeLock and Blue Coat, we were dealing with nine different data centres in different locations. We knew we could optimize that infrastructure sprawl.

When we first considered public cloud, we started with the consumer business. That allowed us to see how the process would work without having to move the entire organization to the cloud at once. Moving data and applications to the cloud is difficult because the cloud will not exactly mirror the current landscape. In most companies, legacy infrastructure exists, and you can use a move to public cloud as a catalyst to clean up some of that technical debt, horizontal scaling, and obsolete technology.

In our migration, we mapped all the workloads that supported consumer business—everything from e-commerce to legal applications, Jira, and other engineering applications. In total, there were about 200 workloads that we categorized by colour. Green meant relatively easy to move to public cloud. Yellow meant moderately difficult. Red meant custom-built, often a legacy application. Finally, grey meant significant risk to move to the cloud

Despite having workloads in all these categories, we were able to move the majority of consumer business to the public cloud in less than eighteen months. How? First, we had the right motivation internally after understanding our risk profile. Second, we had the right partner. This was a joint initiative between IT and the consumer business unit. We were all in this together. We established a cloud council, regular check-ins, and significant communication

with Microsoft, our cloud partner, who helped us along the way.

The migration of our apps to the cloud was an incredible learning experience for the entire organization, not only IT. Now that Symantec has moved all its apps, we plan to spend another year optimizing. That will ensure we are leveraging cloud resources efficiently. We also will be "dialing the knobs" to make sure each application is optimally leveraging this new infrastructure.

When an organization moves an app to the cloud, it also must investigate the dependencies of the app, its scalability, and any capacity needs. Also, it needs to "cloudify" the app as much as possible to take advantage of cloud capabilities (auto scaling, loosely coupled architecture, etc.). Most older apps, especially those that were homegrown, don't work "smartly" out of the box in a new infrastructure like public cloud. You can choose to refactor the application to become smarter before the migration, or you can, as we did, first make the shift and then optimize after finishing the cloud migration.

The good news is that optimizing applications in the cloud is easy to do with the latest tools and technology. You can allocate the minimum resources for the application to run in the cloud and scale them based on the demand and usage. You have the flexibility to adjust compute,

storage, and network resources, and optimize the costs effectively. You need to have a strong governance model to manage the cost structure. Each case will be different, and monitoring is essential.

Our cross-functional cloud council drove the adoption of our cloud strategy as well as the ongoing optimization of our cloud footprint. Real-time dashboards now track and report financials, availability, and performance. Security KPIs are measured across three dimensions: cloud migrations, operational service quality, and capability maturity. These dashboards are used effectively to ensure ongoing operational and executive governance.

In public cloud, the cloud providers only offer security up to the IaaS layer, and the customer must protect their resources (operating system, storage, network policy, identity management, access, and data and application security). We built core services and security tools in a hub-and-spoke model and gave access via a federated access model to various tenants in the hub-and-spoke model. This eliminated the need to create redundant services and tools in the public cloud. At Symantec, we leverage our products to secure the workloads in public cloud. We use Symantec Endpoint Protection (SEP), Data Center Security (DCS), Control Compliance Suite (CCS), Cloud Workload Protection (CWP), Web Site Security (WSS), Data Loss Prevention (DLP), and Cloud Access

Security Broker (CASB) to protect our cloud resources, common resources, data, and applications. The transition to public cloud supported the organization in three major ways. First, it significantly reduced our costs. We were able to decommission nine data centres globally. Second, it improved our security posture. We no longer have legacy data centres around the globe, we eliminated the technical debt, and we leveraged Symantec security products and solutions to protect our workloads, resources, and applications. Third, it increased our speed to market.

THE PROCESS OF MOVING TO NEW TECHNOLOGY

You can move quickly to adopt SaaS and IaaS into your operations, though it's important to understand why you are investing time and money in this migration in the first place. So, step back and consider what you are trying to accomplish by answering these questions:

- What is your risk profile?
- Do you have a crisis you are trying to respond to?
- Are you simply trying to learn and test?
- Are you moving because it is the popular thing to do, without a clear plan in place?

Your answers will inform your decision-making, but whatever your approach, you will need the right partner to keep

things on track and provide the necessary hand-holding along the way.

LOOKING FOR THE RIGHT PARTNERSHIP, BOTH INTERNALLY AND EXTERNALLY

CIOs don't have the luxury of spending time working with multiple "one-off" vendors. Instead, they try to strike strong partnerships with just a few organizations and they choose carefully. And choose carefully. When it comes to moving to a new technology, the right partnership makes all the difference. We chose Microsoft Azure to help us with our migration, and we use Amazon's AWS for other parts of our organization. Both partnerships have been great experiences.

A CIO is responsible for the technology that sits in the company—from data centres and servers to laptops and phones. Creating these external partnerships is essential. They can educate and train your teams on the latest technology and guide you through the process, as they have had other customers go through similar journeys. If you approach vendors for one point solution, you run the risk that the solution might become outdated three months later. When you work with a partner that understands your business and where you are headed, they can offer global support and solutions that will grow with your organization.

Your partner will need your assistance to make sure everything runs smoothly. So, if you ask a vendor for enhanced security requirements, expect them to tell you what they need to make it happen.

The right partners will always be customer-focused, doing everything in their power to drive your company forward. Get to know the team assigned to work with you as well as their executives. In a crunch or a crisis, the right relationship will make the otherwise impossible, possible.

Symantec has lowered its costs thanks to our adoption of SaaS, IaaS, and the cloud. We didn't get there overnight. Therefore, set expectations if you do decide to migrate. You will initially encounter what I call a "double bubble" cost. You will pay for the transition while also paying to stay afloat with your current infrastructure. Rest assured, though, it's only a temporary stage. When the organization reaches the point where you begin to optimize, you'll start to realize a significant cost benefit.

Cost-planning is a vital part of the process, and it's important to foster clear communication across the organization. Every six weeks, for example, I sit down with my business partner, who also happens to be the general manager of the consumer business unit. Our teams conduct a joint meeting that assesses the state of the migration and the cost structure. We also brainstorm how we can innovate

further. The alignment of business and IT helps both teams understand the bigger picture, particularly as it affects cost, agility, and time to market.

A NOTE ON TEAMS

As some functions in IT are increasingly managed by this new technology trifecta, we must re-evaluate how our teams look and function. What does change mean for employees when their jobs look different now than they did a year ago? More than ever, it is essential that we keep our top talent so that capable team members can transition to new functions and support change and growth within the company. Unfortunately, everyone now struggles with a chronic talent shortage where the gap between need and qualified IT personnel is widening.

So, what should a CIO look for in a prospective hire? First, an IT professional must be comfortable with change. If they can't handle how quickly everything is moving, they're wrong for the job. A great IT team should be able to stay current and constantly challenge the status quo. So, if an Apple iPhone X can do facial ID recognition, we may ask why we can't have facial recognition on all our applications. Or why can't we get rid of passwords. As new technology comes in, we are constantly thinking like this. Second, keep in mind the fact that most IT people take on their role with the goal of helping business partners.

Think of us as belonging to a broader service organization. Someone who loves to service the business and embraces change is someone with the exact attributes you want on your team.

Over the years, I've revisited my earlier conviction that each person on the IT team should have a focus. I used to believe that there ought to be a separate "infrastructure person," a separate "application person," and a separate "data person." I also thought that they ought to remain in their own organizational silos. No longer. I've had enough experience building several IT organizations since then, and it's taught me that it's better to hire so-called athletes rather than to go after position players. Borrowing upon the sports analogy, athletes are great at what they do, but they also can rotate to other responsibilities when needed. That's why Symantec has implemented a rotation program, where our people are able to contribute by playing several positions.

One way I think of my job is to develop as many CIOs as possible. Why? Someone can only become a CIO after they have logged broad-based experience. If my team learns to grasp all facets of IT, I have essentially developed CIO-thinking athletes who see globally; they understand dependency thinking and how things are tied together across the organization.

We can only offer solutions when we understand how

everything operates and runs. That's why I prize the fact that the IT team is one of the few functions in the company that's able to see horizontally. Most other departments—whether we're talking about marketing, sales, or engineering—have deep vertical expertise. But IT is the glue that keeps everything together, so we must consider business processes as we look for gaps or redundancy across the organization.

SECURITY

A CIO must think about security at every layer of the entire IT infrastructure. Even with all the advancements in technology, I still need to make sure our own environment is secured with the right products. Likewise, I must ensure that the technology we use is protected and secured.

The good news is that most large SaaS, IaaS, and cloud partners provide basic levels of security. CIOs must be willing to trust vendors to do their jobs. So, if an application goes down, for example, it is the vendor's responsibility to get it back up.

But if we're to trust vendors, our perception of security will have to evolve. Vendors specialize and support thousands of companies. Their infrastructure and service in their areas of expertise are going to be better than any single company because they work with thousands of customers.

The prospect of ceding some control sounds scary at first. But if we can gain a more realistic perspective about what that means, trust should not be an issue.

In all partnerships, security should still be top of mind. In the past, customers ran their own data centres. Now five thousand customers run in one SaaS provider, thus making security even more critical. It's essential to know how the data is segmented, secured, and transferred.

Along with normal service level agreements (SLAs), it's now standard to have security SLAs because of the many expectations around security. A partner's security posture should be known before entering into any agreement.

SECURITY AS A SERVICE

For all the help extended by new technologies, the task of managing security remains complex and difficult. CIOs have more to think about than ever. Why wouldn't they want to have experts at the security level do some of the thinking on their behalf? Today, it is possible to buy and run security as a managed service. Just like cloud, Security as a Service (SECaaS) is simply the way things are going.

Multiple layers of threat prevention, detection, and forensic technologies provide a complete view of malicious activities across control points, so all instances of a threat

can be contained, investigated, and remediated. Encryption, data loss prevention, multi-factor authentication, tagging, and analytics ensure that confidential information and IT assets are protected and in compliance always, wherever they are stored, and that only authenticated users can gain access.

In IT, your infrastructure consists of all your endpoints. It includes everything that is happening with the data, applications, and network. In every layer of this infrastructure today, there are cloud offerings. If everything is a cloud offering, and data is moving fluidly from infrastructure to applications and IoT devices back to infrastructure, why wouldn't security be offered as a service as well? If everything is moving to cloud, why wouldn't we want to wrap security around everything that is in the cloud? As Symantec moves to cloud, SECaaS will become our central offering.

SECaaS also helps you stay close to the data. At the end of the day, security is a data problem; data is what we're trying to protect. We can't protect all the data, but we do need to protect what is most important. The most important data for you might be your PCI information. In our case, it's the intellectual property our engineers generate. No matter what it is, security must be close to that data, wherever it is flowing. If the data is flowing through public cloud or SaaS applications, you want to make sure that all of it is 100 percent secured.

With all the change happening in the cybersecurity space, the nefarious actors are also getting smarter. In fact, they make a living by getting smarter. This adversary makes the job of the CISO incredibly difficult. The bad guys find ways to get in, watch for a while, and then move forward with highly targeted attacks.

Considering this reality, advanced security technologies are more needed today. The earlier you can detect a threat, the easier it is to avoid any issue.

CHAPTER 2

BUILDING A SELF-DEFENDING NETWORK

JEFF STARK: VP, TECHNOLOGY RISK AND CISO, IGM FINANCIAL

Jeff Stark has over twenty years of experience in the IT and cybersecurity industries, including work at ING Direct Canada (now part of Scotiabank), Bank of Tokyo-Mitsubishi UFJ Canada, Canadian Imperial Bank of Commerce, the Ontario Pension Board, and Investors Group Mackenzie Financial. In that span, Jeff has focused on deploying innovative solutions rather than upholding old standards and designing security systems that empower organizations to take a proactive—rather than reactive—approach to data security while maintaining the highest standard of usability and protection.

Technology has advanced to the point where machine learning and the potential for artificial intelligence give us an opportunity to respond dynamically to an ever-changing threat surface or threat vector. These are considerations that security professionals should take into account as they build out their security framework. We are not far from the day when our networks will be able to adapt automatically and respond to

threats as they present themselves—maybe even before they present themselves. —Ajay K. Sood

For years, a belief has persisted that it's impossible to totally defend an enterprise network, that it's not a matter of *if* a network will be breached, but *when*. This mindset has permeated the security industry, travelling through the rank-and-file employees in the IT department all the way to the chief information officer (CIO).

However, such a widespread assumption that breaches aren't avoidable, but rather inevitable, begs the question: When did we give up as security professionals? Is building a defensible network really so hard that it can never be done?

Just as no one buys car insurance expecting to get into an accident the next day, no security professional should approach their job as if they've already failed. This mindset is not only wrong but also counterproductive, causing organizations and security professionals to pay attention to the wrong areas. Instead of focusing on what they can do to build a defensible network, organizations spend far more time planning their responses to a breach.

It's both cheaper and easier to prevent a data breach than to respond to one. If organizations can learn to shift back to a mindset of prevention rather than response, a position

in which they prepare for the worst but expect the best, they will have taken a significant step toward implementing more proactive security solutions.

This chapter explores the evolving landscape of security tools, and how emerging technologies driven by machine learning can be used to create nuanced, adaptive, self-defending networks that put control back in the hands of the enterprise.

To adapt to this new environment, the modern security professional wears three hats:

1. **The security hat**, which allows them to understand the risks of emerging technologies.
2. **The business hat**, which allows them to understand the business needs driving the adoption process.
3. **The marketing hat**, which allows them to sell their proposed IT solutions to the rest of the organization, namely the C-level executives, and build a mutually beneficial partnership.

Security can't be seen as operating in its own world anymore. Those in security and IT who don't understand their business can't do their jobs properly. To be effective, professionals must shift their mindset from gatekeeper to enabler, partnering with their company to ensure the organization can meet its goals safely and effectively.

THE RISE OF THE SELF-DEFENDING NETWORK

Modern attacks to enterprise security systems are happening more rapidly and with more variants than ever before. They're happening so rapidly, in fact, that the traditional human-led response model is no longer adequate. Too many alerts from too many devices are generating too much data for even a well-staffed team of security experts to keep up with. By the time the analysts have a chance to pull all the data together and construct a clear picture of a breach event, the damage is already done.

A new generation of tools has emerged to meet this challenge. In the event of an attack, instead of raising an alarm for their human counterparts to investigate, these systems can respond automatically and counter the threat. With these tools, an alarm that generally takes hours, days, or months for a human analyst to review can now be resolved in near real time.

THE PROMISE OF MACHINE LEARNING

Self-defending networks rely on machine learning to be effective. This is a critical distinction from previous approaches to security, allowing for real-time responses to threats. Their highly advanced algorithms are able to learn what constitutes normal activities within the network and then respond instantly to any deviation.

For instance, Jeff the employee could come to his desk every day at nine o'clock, log in, check his email for about twenty minutes, check his bank account, and then set about his work. The self-defending network would learn this behaviour, so if one day Jeff logs into his system at three in the morning, pulls up the company's customer database, and tries to download data, a series of red flags would be raised.

The system's response in this situation is largely determined by whatever controls the security team puts in. It could block Jeff entirely if his role prevents him from accessing such sensitive data, or it could require further verification before allowing him to proceed. Whatever the case, unlike a human-driven system, a self-defending network is able to detect any abnormal behaviour immediately and respond effectively to any potential attack.

BARRIERS TO ADOPTION

Despite their clear value, many organizations are hesitant to deploy the kinds of self-defending systems I've described for fear of how end users—namely, their employees—might respond to the introduction of a system that monitors their behaviour. Such concerns are understandable, but they can also be overcome through effective internal marketing. Organizations must communicate that, yes, they may be monitoring their employees' activity,

but only in aggregate for the purposes of monitoring the overall behaviour of the network, not for scrutinizing an individual's day-to-day habits.

For example, if Bob has a tendency to hop on Facebook after lunch, the system would learn this, but that information wouldn't factor into Bob's next employee review. Neither these self-defending networks nor the security analysts who run them are interested in Bob's Facebook habits. Instead, they're interested in anomalies. The only time Bob's Facebook usage would matter is if it coincided with a potentially dangerous deviation in behaviour. If Bob decided to upload confidential client data to Facebook, for instance, the network would respond in whatever way the security team had programmed it to.

Through this process, these self-defending networks gradually build profiles of how a typical person might act within an organization. Whether an employee works in HR, sales, or a customer service call centre, their behaviours produce a dataset that is combined with and compared against other employees in those departments. The more data these systems collect, the more they're able to build baseline profiles that predict the actions not only of current employees, but of future employees as well. In other words, the system would expect that Barry, the new finance employee, would likely behave similarly to Barbara, a seasoned vet. Through this process, the

system becomes increasingly adept at recognizing and responding to suspicious activity—protecting both the individual and the organization in the process.

One potential drawback to these systems is that they take time to learn the environments in which they operate. These aren't "plug and play" devices that demonstrate immediate returns, but rather tools that will show benefits over time. Organizations considering their adoption must have a clear expectation that it may take months for the system to become effective.

A SHIFT IN THREAT RESPONSE

Traditional network defence tools are inherently reactive, built to protect against known attacks rather than adapt and anticipate attacks in real time. For instance, if a piece of software comes out, attackers will work to identify a vulnerability in that software and write an exploit to take advantage of it. Antivirus companies then detect the exploit and write something called a signature to detect it.

Unfortunately, that signature is only a temporary stop-gap. Once the attacker sees that a signature has been developed, they simply modify their code, creating what's called a variant, to render that signature useless. The antivirus company then updates with a new signature, the attacker counters with another variant, and so on.

After a while, the antivirus company ends up with hundreds, maybe thousands, of signatures, all in response to the same exploit and its variants. As this signature database grows, the antivirus software becomes increasingly resource-intensive, having to check every incoming file against a massive list of potential exploits.

BREAKING THE CYCLE

In order to escape this endless game of cat and mouse, many companies are starting to rethink how they write their signatures. Instead of trying to detect the exploits themselves, they work to detect the characteristics of that exploit instead. Suddenly, a process that once required hundreds or thousands of signatures can now be accomplished in one.

This shift in strategy has helped pave the way for a new generation of security tools that can automatically adapt to threats. For instance, say Company A is breached. The details of that attack are then sent back to the security company's central intelligence operation, where self-defending programs are quickly able to discern the root cause and provide updates to their software. These updates are then sent out to Companies B, C, and D, protecting them from the same attack that worked against Company A. Like a person receiving a vaccine, a form of herd immunity is established by all organizations using

that security tool. Through machine learning and a massive global dataset, security companies are able to protect client data in near real time.

While the benefits are significant, such a process requires a certain amount of trust on the user end, in this case, the enterprise and their security professionals. These professionals need assurances, that (1) their data is safe, and (2) the data they receive won't disrupt the company's network, causing it to block an important business process.

These are legitimate concerns. After all, no company wants to risk a potentially costly interruption to their day-to-day operations. However, the alternative—sticking with traditional, reactive controls—leaves them far more vulnerable to a breach in an era of increasingly sophisticated attacks.

Given a choice, most security professionals would choose the former option, preferring the occasional interruption to day-to-day business over a needlessly vulnerable network. However, the decision doesn't rest with them, but rather with the decision-makers in the C-suite. To secure buy-in, the security professional must adapt the mindset of facilitator rather than gatekeeper, explaining that an adaptive network is a non-disruptive business solution with the least amount of risk.

BEST PRACTICES FOR A HYPERSCALE NETWORK

Another major consideration for the modern security professional is the rise of the hyperscale network in the form of cloud computing. Most enterprises see cloud computing as the next evolution for their business, offering savings in both everyday operations and specifically in overall IT cost. When compared to traditional, server-based solutions, the cloud offers both flexibility and improved speed of deployment. Servers traditionally take months to deploy—from hardware delivery to installation to rollout. With the cloud, businesses can be up and running with the same capabilities in minutes.

From a business perspective, the cloud offers businesses a host of solutions with no apparent drawbacks—that is, except for the attendant security risks of trusting company data with a third-party provider. From an IT perspective, the idea that the marketing department, for instance, can bypass internal servers, safeguards, and regulatory requirements by migrating their campaigns to the cloud can be terrifying. Equally terrifying to the marketing department, however, is not having the freedom and resources to launch a modern campaign speedily.

Traditionally, security and IT professionals have known exactly how many servers they had and where they were located, allowing them considerable control of the ingress and egress points within their firewalls. With the cloud,

that kind of fixed location—and the peace of mind that comes with it—is gone. IT no longer knows how many systems are housing their workloads, or even where those workloads are, since most cloud-based providers like Microsoft, Amazon Web Services (AWS), or Google move their workloads to different locations depending on factors like power rate and even time of day, and they are under no obligation to notify IT when they do this.

Further complicating the cloud adoption conversation is the fact that multiple competing cloud-based services exist, and each is trying to undercut the other on price. For example, Business A may be happy paying $1.99 a day for Amazon Web Services, but one day they notice Google is offering the same service for $0.50 a day. Suddenly, Business A wants to move their entire workload from Amazon to Google to take advantage of those savings.

This is the promise of the cloud, and it's an enticing one. Traditionally, switching manually from server to server would have been time-consuming, costly, and somewhat risky. However, with cloud computing, the switch can be painless and almost instantaneous.

To account for this, security profiles must be designed to automatically travel with their workloads. Such a process represents a complete break from the traditional practices of the past twenty-plus years. However, the changing

needs of enterprise computing demand a change in how we think of information security. That said, anytime massive amounts of confidential company data are changing hands, IT has to ensure that these data are safe. Security professionals must work toward designing automated security solutions that can wrap around their business's workload and move safely either within the same cloud or across clouds to a different provider—while still maintaining the same level of security as an on-premise solution, and with no negative impact to business process.

ACCOUNTING FOR ELASTICITY

The other enticing promise of the cloud is the elasticity of the services provided. Platforms like AWS can adapt to changes in demand, expanding and contracting the number of servers allocated for a business based on its needs. This is particularly beneficial if, for instance, a company starts generating more web traffic around the holidays. Whereas two servers used to be enough to do the job, the moment they become insufficient, AWS can automatically grow the number of systems on the back-end to support the increased workload.

The challenge for security professionals is to ensure that when each new server comes online, their data remains protected. To do this, they must design a security profile or policy that grows and shrinks with the cloud—and without

human intervention. The security piece must have the same autonomy to adapt as the cloud itself. Otherwise, the IT department will be left scrambling to manually apply safeguards every time the server count changes.

THE GROWING PHENOMENON OF ENCRYPTED TRAFFIC

The final consideration driving the need for self-defending networks is encrypted traffic. According to Gartner, 80 percent of all web traffic will be encrypted by 2019.[2] From the perspective of the end user, that's great news, as more encryption means more privacy. However, from a security perspective, encryption is yet another obstacle to be overcome, as it eliminates all visibility to that traffic—and therefore the ability to protect it.

RUNNING BLIND

This lack of visibility can affect networks in several different ways. In one scenario, a user might make an outbound connection to the internet, perhaps to a banking site or some other web application. Traditionally, as that traffic moves through the network, it's inspected by a firewall and either approved or blocked and scanned for malicious content. However, if that traffic is encrypted, those inspec-

2 "Encrypted Traffic Analytics," Cisco, 2018, https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf

tion tools are blind to the data. All that can be determined is the source of the information and the destination. Such scarce information offers security tools little chance of detecting a malicious payload.

In a traditional environment, security can't do much about encrypted data. By the time the data is decrypted on the web server or client machine, the only line of defence left is the endpoint's antivirus software, which may or may not be equipped to spot and defend against an attack.

This isn't an ideal situation. Many enterprise organizations spend millions of dollars for effective network security solutions, and they aren't thrilled to learn that encrypted traffic is rendering the vast majority of those tools useless. Users, for their part, should rightfully expect a certain level of privacy with their web browsing. However, if that privacy effectively blocks organizations from protecting against external threats, it creates a lose-lose situation.

The goal for security, then, is to have the ability to inspect this encrypted traffic. The most common way to do this is by issuing trusted certificates to the end user's workstation. Typically, when an end user connects to the internet, their data is encrypted as it passes through a firewall or other similar device within the network. To inspect this traffic, the security device will use the trusted certificate to decrypt the data, run it through its inspection tools,

and re-encrypt the data before sending it to the external web server.

As much as the IT department might prefer otherwise, encrypted traffic is here to stay. Google already warns users every time they're visiting a page that isn't encrypted—and the day may come soon when browsers like Chrome only load encrypted traffic.

Here again, the role of the IT department is to play facilitator, to find solutions that open the encryption chain in a way that maintains the trust of their end users. Some concessions likely will need to be made. While security analysts would prefer to look at every piece of data that comes through the network, they also need to assure employees they're not reviewing any private information. Certain regulatory environments, for instance, may limit the types of personal data that can be decrypted, especially information coming from sites categorized as banking, healthcare, or government services. Care must be taken to ensure this type of data remains confidential.

Even now, that capability exists. The challenge, however, is ensuring that website categorizations provided by the vendor are correct and haven't been modified by a malicious actor through a phishing site (e.g., a site mimicking a bank's homepage). If IT is willing to allow certain categorizations to pass through into the network without

being decrypted and inspected, they must have assurances that attackers haven't yet figured out a way to trick those systems and infiltrate the enterprise.

THE MOBILE DEVICE CURVEBALL

Further complicating this discussion is the widespread adoption of mobile devices. For employees on company-issued mobile devices—whether that device is a smartphone, tablet, or laptop—how does the IT department extend these network capabilities to the device so it's protected?

There are multiple approaches, each with varying levels of risk:

1. Control security at the endpoint. This could be traditional antivirus software or newer behavioural-based endpoint solutions backed by the cloud.
2. Connect over a virtual private network (VPN). Every time a mobile system comes online, it automatically connects back to the enterprise's home network, allowing employees to browse through a secure infrastructure and enabling the network's existing toolset.
3. Accept the risk. Although not ideal from a security perspective, an organization may decide they are comfortable accepting the risk of mobile devices within their environments. This decision may be due to lack

of experience securing these devices; perceived cost, both in financial and functionality terms; or not fully understanding the risk these devices pose to the organization.

For companies with a bring-your-own-device (BYOD) policy, there are still more considerations. On one extreme, IT could choose to block all company access through personal devices other than email. However, even allowing that small amount of access has risks, since confidential information such as a driver's licence or passport information is often shared through such channels.

In the modern on-the-go business environment, organizations may find such restrictions unnecessarily prohibitive. Another option is to connect the device to an enterprise-controlled portal, whether in the cloud or hosted in a company-controlled data centre. Through such an approach, the device can access anything the user wants, but all the data and computing are processed externally through the portal. Such an approach has additional benefits if the device is stolen or the employee leaves the company. In this scenario, all IT would have to do to protect their data is delete the user's account.

Another commonly used option is a process called sandboxing. A sandboxed app creates what's called an enclave within the device's operating system where only that appli-

cation and its data can be stored. No data whatsoever can be transferred between the device proper and the applications in the sandbox, which, like the portal, typically connects directly back to the corporate server.

ENVISIONING THE BUSINESS-DRIVEN NETWORK

When it comes to securing data, the typical enterprise has many variables to consider. Ultimately, their decisions must be business-driven. IT and executive leadership must carefully consider what they're trying to accomplish and what experience they're trying to provide their end users while maintaining the trust and privacy of a secure connection. Once those goals are defined, the question of how security professionals might go about decrypting data and scanning it for malicious content becomes much clearer.

There will always be a need for security practitioners. However, their role in the enterprise is changing, forcing them to become more business-focused as they look to create practical, workable solutions that (1) minimize risk, (2) don't violate existing privacy laws, and (3) don't inhibit business processes.

In a typical data loss scenario, the old-school security system takes a binary approach: it will either allow or block an action. For instance, perhaps Deb in marketing

isn't usually supposed to send customer data to Tom in accounting, but in this particular instance, she has been cleared to share this information. While most current systems would block Deb outright, an adaptive system could flash a warning: "What you're attempting to do violates our privacy code. It looks like you're trying to send some customer data. Are you really sure this is what you intended to do?" From there, Deb could confirm her intentions, and the data could either carry forward unimpeded or be forwarded to a manager for approval. This maintains security without unnecessarily impeding business processes.

Championing such nuanced, granular processes would produce benefits across the organization. In recruiting, for example, it could mean the difference between finding a highly qualified candidate and a mediocre one. If the resumé of a highly qualified candidate is blocked because it somehow managed to pick up a virus, this might be a win for security, but it's a loss for HR, who just lost their best candidate—and they didn't even know.

In the new reality of the self-defending network, when that same malicious email from that same qualified candidate comes in, security could inspect it, strip the malicious content, and forward a clean version of that resumé to HR. Such a scenario is a win-win for everyone. Not only is security doing their job, but they didn't break the busi-

ness process. In fact, they supported it, enabling the best candidate to connect with the company.

The days of the self-contained, server-based enterprise are numbered. As more enterprises move their operations to the cloud and adopt mobile workstations, security practitioners must adapt to a changing environment by embracing a big-picture approach. What does their business want to accomplish? How can security enable those goals while keeping the business safe?

To keep pace with a constantly evolving space, tomorrow's security solutions need to be proactive rather than reactive. They must be capable of anticipating and blocking attacks in real time without inhibiting the activities of the end user. Balancing all these concerns will sometimes feel like walking a tightrope. However, practitioners can help relieve these concerns and improve the conversation surrounding data security by involving the end user in the process.

This change in approaches can be likened to a change from the passive, reactive responses of a traffic cop to the active, investigative approach of a border patrol officer. The traffic cop takes a binary approach to security—either a person is speeding or not—and moves only to block those in clear violation. The border patrol officer, however, asks questions before coming to a conclusion. They

understand that even a seemingly harmless family station wagon could be smuggling contraband.

This is the context in which the next wave of network security will flourish. By taking a more active role in the inspection process, security professionals are able to better protect the flow of incoming or outgoing traffic while simultaneously enabling, rather than inhibiting, business processes. However, security can't accomplish this alone. For modern enterprises to embrace the new reality of data security, they must evolve their mindset from gatekeeper to enabler, from yes-or-no responses to nuanced approaches that take both the business's and the end user's best interests into account.

CHAPTER 3

COACHING YOUR BOARD AND LEADERSHIP PEERS ON CYBERSECURITY ISSUES

AMIR BELKHELLADI: PARTNER, RISK ADVISORY LEADER FOR EASTERN CANADA, DELOITTE

Amir leads Deloitte Canada Eastern Region's Risk Advisory practice and has nearly twenty years of experience in cybersecurity, focusing on strategic advice and leadership of significant global cybersecurity transformation programs. Amir previously worked in France, where he led Accenture's security practice, and in the UK as the chief security architect and group operations chief technology officer for Lloyds Bank, the country's largest retail financial institution.

Gone are the days where cybersecurity was considered to be just an IT problem. Board-level and executive-level awareness are no longer optional—they are essential. At every level of government or enterprise, some understanding of cyberattacks as a threat to business or service continuity is required.

Just ten years ago, roles like chief security officer (CSO), chief

information security officer (CISO), and chief risk officer (CRO) either didn't exist or had a very different set of responsibilities that did not involve cyber. Today, they almost exclusively involve cyber. Furthermore, all of these roles are in a process of rapid evolution. —Ajay K. Sood

Cyber-enabled risk is one of the highest threats that organizations face today. For the last ten years at Deloitte Canada, I have worked with global financial services companies, every one of which ranks cyber risk among its top ten most serious threats. It is a risk that boards of directors and senior leaders absolutely must know about, understand, and take serious measures to combat.

Cyber-enabled risk truly is an existential threat to many companies. For example, we worked with one of the largest financial institutions in the world. They had a virtually unlimited budget for cybersecurity and they invested heavily in protecting their clients' money from cyberattacks. Yet the CEO still identified cyber risk as the number one existential threat to the institution. If a financial services company of that size, and with that power and a virtually unlimited budget, considers cyber risk to be an existential threat, then many other companies would be wise to do the same.

A big part of what every board does is identify threats to the company and address them appropriately. Boards

don't have operational accountability—that's the job of the CEO and the management team. But the board has oversight responsibility of the CEO and management. In that role, the board must understand all risk the business is facing, whether it's competitive, strategic, financial, or cyber.

It is the job of every board member to understand cyber-enabled risk. If they don't grasp that risk now, it is incumbent upon them to spend the time to learn about cyber risk, educate themselves, and ask for additional training, resources, or support to get their mind around what cyber risk means to the organization. Only when the board understands cyber risk can they take steps to mitigate it effectively, monitor it, and make sure it falls within the board's risk appetite. The truth is that no organization, no matter what they do, can eliminate cyber risk 100 percent. There is always a chance that a company will be breached, even if only through human error or carelessness. Every organization, usually at the CEO or board level, must decide what level of risk they find acceptable. The board is usually the body that decides an organization's risk appetite. If any threats fall outside of the acceptable level of risk, action must be taken.

CHANGING TIMES

Ten years ago, many boards either did not know about

cyber-enabled risk, or they knew about it but did not take any action to mitigate it. Today that has changed. Every board knows about it. They read about it every week in the news. They hear about companies being embarrassed and brought to their knees because of a breach. Yet not every board takes it as seriously as they should.

Most boards of directors are not composed of people with a cybersecurity background. Cyber is not their area of expertise. Board members typically have expertise in areas like finance, operations, manufacturing, sales, or innovation. Very few come from the cyber world—although that is slowly changing.

Therefore, most boards find themselves with a limited knowledge base around cybersecurity risks. Their first priority should be to educate themselves on the broader cybersecurity risk environment. Their second priority should be determining how cyber risk specifically affects their organization, and where the vulnerabilities are. It could be that private customer data is vulnerable, or company banking records, or employee information, or trade secrets, or even information held by vendors in the supply chain. Each company has different risks and vulnerabilities. Their third priority should be determining how best to mitigate those risks.

THE ROLE OF THE CHIEF INFORMATION SECURITY OFFICER (CISO)

The CISO is typically the position that acts as a liaison between the cybersecurity team and the board of directors. The CISO will brief the board on cyber threats, risk assessment, and generally be the person who requests a budget to mitigate those risks. It is a challenging role and requires two important skillsets.

The first skillset of the CISO is technical knowledge and expertise. A CISO must have an excellent understanding of the technical side of cybersecurity. A CISO must understand the technology and the tools used to defend against an attack, and to protect the organization's data.

The second skillset that an effective CISO must possess is broad business knowledge and experience, which results in the ability to understand how cyber affects core business operations. It's not enough for a CISO just to understand the technical tools and how to patch holes; a CISO must also understand and be able to communicate the effects cybersecurity and cyber threats can have on the day-to-day operation of the business. Furthermore, a great CISO has to be able to help the board and senior management understand cyber risks and convince them on why and how the requested budget for cyber will directly benefit business operations.

THE CISO MUST FOCUS ON IMPACTS TO THE BUSINESS

Imagine the software system running a manufacturing line gets hacked and goes down for a week. The CISO doesn't need to make the board understand the details of how the attack happened. But the CISO must be able to communicate to the board that every minute that line is not producing product, trucks are waiting empty, raw materials and parts are piling up, the supply chain is backing up, and customers are not buying. Every hour that situation persists is costing the company money. An effective CISO will help the board understand that.

Here's a real-world example—from before I joined Deloitte, when I was working under the CISO at a large bank in England. We identified a security gap, so I asked the CISO if I could present it to the board and ask them for the budget needed to fix it. The CISO said yes, but warned me not to get my hopes up because the board had always said no when the CISO asked for additional budget for cyber.

I went into a board meeting and presented the risk, then I detailed exactly how it would have tangible and potentially devastating effects on the core business functions of the bank if we didn't spend money on a solution. In my presentation, I did not focus on the technical tools that were needed; I focused on the business risks. The board approved the budget I requested.

I convinced them of the business need by speaking in terms they understood.

This is a powerful example of how a CISO must learn to speak to the board in terms of core business operations and strategy so that they will understand and take action.

Part of working with a board is knowing how much—or how little—technical detail to present. When I coach boards about cyber-enabled risk, I keep the discussion at the 30,000-foot level. I refrain from going through ground-level technical details of how cyberattacks happen, what kinds of threats are out there, or the technical details of processes and tools that can help prevent an attack. The board doesn't need to know all that. They think at a big-picture level, and they think about profit and loss from business operations.

When dealing with a board, a CISO should focus on two main areas: the potential impact of an attack and the likelihood of an attack happening. A high-level approach with the board works because cyberattacks almost always result in a major business impact or a reputational impact that can slow down or even derail the company's overall strategy. Board members will understand that, but the CISO will have to spell it out for them clearly. Boards think in terms of business impacts much more readily than they understand the technical side of the cyber issue.

WHO IS ACCOUNTABLE?

A big question that must be addressed with the board of directors is who is accountable. Usually, you will want at least one person on the board to be accountable for cyber, so this person can be your representative and your champion. However, everyone on the board is responsible, from a good governance perspective, to ensure that cyber risk is under control and mitigated to the greatest degree in relation to the resources available.

Most board members fall into one of three groups. The first group is made up of executives from the company, such as the CEO, usually the CFO, maybe some VPs, and rarely the CIO or CISO. They represent the management of the company on the board. The second group on the board is made up of owners or large shareholders in the company, or their representatives. The third group is typically filled with non-executive directors, or NEDs. These are independent board members who do not work for the company but have expertise in various areas of business and who will help the organization make sound decisions. For example, Bob Iger is on the board of Apple, Inc., even though he is the chairman and CEO of The Walt Disney Company.

The most advanced organizations will hire non-executive directors for their specific cybersecurity backgrounds to compensate for the other board members' gaps in under-

standing. This trend is another sign that companies are recognizing how serious cyber threats are.

BOARDS AND THE CHANGING REGULATORY ENVIRONMENT (GDPR)

The board of directors has an important role in overseeing compliance with increasingly complicated regulations and laws governing cybersecurity and breaches of private information. These laws vary widely by country and industry, as well as by how many employees an organization has.

2018 saw a massive shift in the level of accountability that companies must have when it comes to protecting their employees' and customers' private personal data. In the European Union in particular, the laws are changing and the potential consequences are enormous. Boards must fully understand these major changes in the regulatory environment.

On May 25, 2018, after a two-year grace period, the European law known as the General Data Protection Regulation (GDPR) went into effect. The GDPR is a complicated, wide-ranging law designed to protect people's personal information. It will affect companies inside and outside the EU. Perhaps the most notable aspect of the GDPR from a board perspective is that it allows for massive penalties

for companies who fail to meet its requirements. You will find a fuller discussion of the GDPR in Chapter 12.

Companies have always had to worry about data breaches. In the past, organizations mostly worried about the negative reputational impact caused by a breach. Today, they're concerned about reputation damage *and* the millions of euros in potential fines and penalties. The fines under the GDPR could go well into the tens of millions of euros, and potentially much more: the maximum fine is up to 4 percent of the company's annual turnover. You can do the math on that one. The fines are potentially much, much bigger with the GDPR than with older laws. Under past regulations, organizations had to be compliant, but there were no sharp teeth. That's all changed with the GDPR. It's so serious that every board member must know the basics of the GDPR.

Ultimately, the board has direct accountability to the GDPR regulatory agency. Not only do boards need to be aware of the law, they must also make sure company management is complying fully with the strict new regulations. Because the GDPR is designed to protect private individuals' personal data, it has shifted the conversation and the responsibility dramatically. Before the GDPR, companies checked off the boxes to be compliant with current law, but under the GDPR the regulatory agency is actively security testing companies and evaluating how

effectively they respond to an attack. This is a massive paradigm shift.

Boards need to know where their data is stored and that it's being handled and protected properly. If the company is collecting personal information, the board needs to know how it's being used and stored. Again, I do not recommend going into technical detail about the GDPR with the board. But the cybersecurity manager or CISO must provide the board with an overview of how data is collected, used, stored, and destroyed.

The good news is the prudent practices that organizations should be doing anyway to protect private information are the same practices now required by the GDPR.

A good CISO will make sure that the board is briefed on and understands the GDPR requirements. The key here is to help the board understand the likelihood that a breach in violation of the GDPR could happen. What are management and the board doing to protect the company against such a breach? What is the plan moving forward? Are we within our risk appetite when it comes to the GDPR? If we are outside the company's risk appetite, what is the plan to fix it?

HOW OFTEN TO DISCUSS CYBER WITH THE BOARD

The CISO, or the cybersecurity manager in a smaller company, should meet regularly with the board. Giving the board a cyber briefing once a year is not enough. In my experience, most successful organizations have a standing invitation for the CISO or CIO to attend board meetings at regular intervals. The goal of the CISO is to bring the board up to speed on cybersecurity and regulatory compliance and, if appropriate, discuss the current security intelligence report. What threats are likely coming in the future? How is the GDPR being implemented? What companies have been fined, how much, and why? How can we avoid a similar fate?

In my position with Deloitte, I either sit on boards of large financial institutions or I act as their CISO. At most large banks, the CISO gives a cybersecurity brief to the board at least once a quarter. Quarterly cyber briefings are frequent enough to stay current, and far enough apart to give the board time to make progress on the issues. If the environment changes and the threat level is particularly high, more frequent meetings should be considered. Some organizations have a thirty- to forty-five-minute cyber brief at every board meeting. That seems to be the sweet spot at many companies. In any case, the CISO should present the current state of cyber and talk about the journey ahead in a cybersecurity briefing.

THE CYBERSECURITY BRIEFING

Each time the CISO briefs the board, there are three things that should always be on the agenda. The first one I call the security posture, which refers to the company's current operational status on security. Have there been any breaches? Have we had any security issues or problems? Were there any direct cyberattacks, and were they successful? What effect did the attack have on the company's operations?

The second point the CISO will want to cover is the cyber program. This is a current assessment of what the organization is doing to combat and prevent cyberattacks. Most organizations today feel that their current security is not strong enough to put them within the risk appetite they have established, and they want to improve it. Briefing the board on the cyber program includes an update on where this stands.

The third element is a look into the future. What's coming ahead in the world of cybersecurity? This could include adding additional cyber staff or new hires in the department, new equipment, and anything external that is happening in the next twelve months. This could also include new regulatory requirements, changes to compliance, new threats, or any other challenges that the board should know about.

CALCULATING RESIDUAL RISK

Residual risk is something the board will want to know about. Risk is generally calculated by multiplying the likelihood of a certain event happening by the magnitude of the impact of the event. Residual risk is the quantifiable amount of risk that remains after taking the appropriate steps to mitigate that risk. In other words, the CISO might tell the board, "Here is a risk we have identified. Here is what we've done to mitigate it. So, this is the amount of risk we're left with after implementing our mitigation plan."

It is then up to the board to decide whether that residual risk is within the risk appetite established by the board. If it's not, then additional steps such as putting new security tools in place, adding more resources, or even buying cyberattack insurance will be necessary. Insurance won't reduce the risk, but it will provide some protection against the impact of a breach.

The real risk comes after you implement protective measures. How long will that residual risk continue? Will it get worse? Oftentimes with risk it's not what you see at first, it's what you don't see.

LEADERSHIP PEERS

As I've discussed, when coaching the board on cyberse-

curity issues, keep your presentation at a high level. Don't get bogged down in the weeds and don't get too technical. However, when coaching your peers—other executives, leaders, and department heads in the company—go granular. You should go into much more operational detail with this latter group.

For example, to understand what risk you're taking, management must understand what their key assets are. As the head of security, you don't have complete knowledge of everything in every department in your organization. But they do. Your peers will know what assets need to be protected in their departments. You will have to work with department heads to identify and reduce risk to those assets. Since working with leadership peers will occur on a much more granular level, the CISO will in many ways become a cybersecurity coach.

Briefing boards and coaching peers is a fulfilling part of the job for any CISO. If you've never done it, you should look forward to it, rather than avoid it. The board is the seat of power in the organization; interacting with board members is a rewarding experience. Know that they will be grateful for your help, wisdom, and experience.

CHAPTER 4

DEALING WITH THE SHORTAGE OF CYBERSECURITY TALENT

EDWARD KILEDJIAN: VP OF INFORMATION SECURITY, COMPLIANCE AND CISO, OPENTEXT

Edward Kiledjian is the VP of information security, compliance and CISO at OpenText, a global enterprise information services firm with 140 offices around the world. Ed has spent the last twenty-five years in cybersecurity or, as he says, since "long before the industry was cool." He has helped secure organizations in more than forty countries and in a wide range of industries, including transportation, utilities, manufacturing, and government. For more of his insights and opinions on security, check out his blog at Kiledjian.com.

It's no secret that cyber talent is in high demand today. What isn't as well-known is why. Certainly, cybersecurity professionals can be trained, and many are graduating from excellent college and university programs that focus on cyber. But it takes more than classroom training for a cybersecurity professional to become fully effective. To put it bluntly, they have to be battle-tested. They need experience on the front lines.

Think of it like this: competent cybersecurity professionals must be created. The best organizations have built a system by which these individuals are attracted, recruited, hired, trained, tested, maintained, supported, and retrained continuously. Why? There's really no other way, because the landscape is so dynamic. This process is a huge challenge for any organization. —Ajay K. Sood

Imagine a constantly understaffed hospital that couldn't hire and keep enough doctors and nurses to meet patient needs. Or imagine the effect a shortage of engineers and rocket scientists would have on a company like SpaceX. What would happen to the major airlines if a lack of experienced pilots caused hundreds of flights to be grounded because there was no one to fly the planes?

Each of these fictional scenarios would create untold hardship and disruption in those industries. Without enough qualified, well-trained, and experienced professional talent to fill key positions, companies are at risk of stunted growth, squandered opportunity, lost shareholder value, and even catastrophic failure.

Such is the case in the cybersecurity field today.

Study after study from reputable organizations, like (ISC)²'s Global Information Security Workforce Study, all say the same thing: critical cybersecurity roles across

all industries remain vacant because of a lack of available talent. Companies of all sizes struggle with recruiting, training, and retaining cybersecurity professionals. Sixty-six percent of companies in the (ISC)² study reported having too few security workers.[3] That shortage leads to serious risks; a study by NTT, the Security Risk:Value Report 2017, found that 52 percent of organizations surveyed do not even have a response plan in place in case of a cyberattack.[4] The problem is going to get worse. The (ISC)² study mentioned above predicted that by the year 2022 there will be a 1.8 million worker shortage worldwide in information security.

Those numbers are disturbing but not surprising. Anyone working in cybersecurity knows the current state of recruiting and retaining talent; it's a massive challenge for organizations, one that can jeopardize their existence. There are too many open jobs and not enough experienced people to fill them. Companies are faced with offering ever-increasing salaries and tailored benefits packages to attract cyber-talent, then working hard to retain those people, who can be poached at any time.

---

3 International Information System Security Certification Consortium (ISC)2, "2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk," Frost and Sullivan, 2017, 3–8, https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf

4 NTT Security, "2017 Risk:Value Report: Business Security: Always a Journey, Never a Destination," Nippon Telegraph and Telephone Corporation, 2017, 6, https://www.nttsecurity.com/docs/librariesprovider3/resources/global_report_risk-value_2017_a4_uea_v6.pdf?sfvrsn=a06281fa_2

Huge demand and low supply means prices skyrocket. The job of the CISO is to hire the best people in order to defend the interests of the company, its customers, its shareholders, and its employees. So CISOs battle this cybersecurity talent shortage every day.

PEOPLE, PROCESS, AND TECHNOLOGY

The holy triad of security is confidentiality, integrity, and availability (CIA). To support that triad, you need people, process, and technology. The technology is the easiest. You write a cheque. You buy some tools. Next, you need to source the expertise to efficiently deploy those tools and then operationalize them and build processes around them. This is the greater challenge. Of course, you need to find the best people to do the work, which is the focus of this chapter.

The first challenge in hiring is that security is a field where you need a broad scope of skills and knowledge in order to be a high-performing technician. That's quite different from being a certified operator of a software suite. For example, if you are a Microsoft specialist you can go out and learn about a specific Microsoft program, do some labs, do some hands-on work, read the manual, pass an exam, and be fairly proficient in that specific software. In contrast, cybersecurity requires a broad range of expertise: you have to be a technical specialist; you have to

have good relationship skills; you must have good communication skills; and in many cases, even if you're not a leader in the organization, you still need some level of managerial skills. That combination takes years to build and is difficult to find.

The second thing that makes finding, keeping, and training people difficult is that security is a fast-changing business. Everything in business is increasing in speed, but the cyber-threat actors are extremely motivated by financial gains, so they're willing to employ the latest techniques, tools, strategies, and methodologies. What that means in security is the skills you acquired two to three years ago no longer apply. Not only do you have to find people with a good skill base, but you also have to find people who are willing to constantly refresh their skillset and stay current.

In short, talent acquisition is difficult. Additionally, retention of this talent is also difficult. Finally, you need to train continuously to make sure that the team's skillsets remain valid.

There's extreme competition for skilled individuals. If you hire a junior or intermediate cybersecurity specialist and you invest in developing that person, the next struggle is giving them what they need to stay with you. There's always going to be a company willing to pay just a little bit more to steal your valuable and skilled resources.

You have to pay your people enough so they don't think about money, then you have to understand what motivates them. That varies widely person to person. For some, the motivation is working with leading-edge technologies and doing things that they find interesting. For others, it's the ability to build a strong network with leaders and executives throughout the business. For still others, it's being able to play the role of expert, representing the organization at conferences and speaking engagements. Once you've hired the right people and you've trained and developed them, figure out how to keep them happy enough that they won't leave.

One of the ways to keep employees engaged and stimulated is through ongoing training. I believe continuous training has to be part of the security team's roadmap. It has to be built into the DNA of the organization. There's a misconception that training has to be a formal classroom-style engagement, but we find that on-the-job training with tools and technologies is more effective and a better value for the organization. Regardless of how it's done, continuous training is an absolute necessity, and the training program should be a mix of classical training (whether that's online or in a classroom) and on-the-job training working with experts. As you bring in your junior people, they have to learn about security, tools, techniques, and strategies from the more senior people. That professional osmosis has to happen as part of a natural evolution of a team.

THE SIX MAIN SECURITY ROLES

Typically, there are six key roles you must recruit for on a cybersecurity team: security tools expert, security analyst, incident responder, automation expert, data scientist, and change manager. Each of these roles has a different function, and therefore requires a different skillset. Many of the skills overlap from role to role but hiring talent for each position will involve recruiting very different personality types.

SECURITY TOOLS EXPERT

These people know the tools and technologies that you have implemented or are planning to implement. They work with your cybersecurity software and systems every day, and they know exactly how to use them for the best results and how to troubleshoot. Tools experts are expensive, but they tend to be more available than some of the other cybersecurity positions we'll touch on later. This is simply because the tools we are dealing with are generally common across industries—many people know how to work with them. If you can't find tools experts, you can train somebody to take on that role within a reasonable timeframe.

Tools experts may be more readily available than other positions on the cybersecurity team, but that does not mean they are less important. In fact, it's quite the

opposite. Such experts are critical to an organization's operations because as tools become more specialized and sophisticated, they require a higher level of expertise to manage, deploy, and operate. For example, consider the security information and event management (SIEM) tool. Think of this as a massive data analytics device. It resides in the middle of your organization and collects security information from all of your different tools, servers, and network equipment. It then correlates all collected data to convert it into useful insights, trying to find the proverbial needle in a haystack. Tools such as SIEMs are easy to acquire, but they're complicated to run because they need to be operated by specialists who have a firm understanding of their operations. Having access to tools experts is the only way for organizations to fully leverage the value of their purchased tools.

The tools expert is a very technical role. The primary qualification is sheer technical expertise. Typically, these are not front-end customer-facing staff, and they don't generally interact with other layers in the organization. This is a good post for someone to begin a career in cybersecurity.

SECURITY ANALYST

The security analyst is a difficult role to fill because it involves a complex skillset. Security analysts are skilled technicians with a good balance of soft skills and busi-

ness acumen. They perform business analysis and make recommendations about how best to secure the organization's data. They understand how the organization works, then figure out how to secure its business processes as a customer, as a service provider, and as an entity.

Typically, security analysts are recruited one of two ways. Organizations can leverage technical experts with good social demeanours and business skills and train them. Alternatively, organizations can recruit business types with above-average technical skills, then provide training on supplemental technical skills.

Security analysts interact with all levels within the organization, from junior business people to executives in the C-suite, partners, and suppliers. This is a difficult role to fill.

INCIDENT RESPONDER

When a breach happens, you'll need a team (or a specialist, depending on the size of the organization) that knows how to use your tools and can also be your crisis management experts. We call this incident response in the security space. Under a live cyberattack scenario, even the most battle-hardened senior executives can get rattled; this is when a trained and experienced incident responder will step up and manage the process.

Incident responders specialize in identifying threats as quickly as possible. They know the tools, they understand the business processes, and they are also risk- and crisis-management experts. They drive tools specialists to retrieve necessary data. They interact with executives and business leaders to collect impact information while providing them with updates. They coordinate actions with other business groups, including legal, finance, and HR.

This skillset is extremely rare. Even though many university programs attempt to teach this subject, my personal experience is that unless someone has lived in the trenches and has performed hands-on crisis management under intense situations, they're not going to be fully effective in real-life crisis situations.

From a training and preparatory perspective, incident responders must continuously test their process. They also need to be constantly trained and drilled so that when the unexpected does happen, the response is so natural that it is automatic, almost reflex-like.

For medium-sized and larger companies, incident responders must deal with an added complexity of managing cyber risk insurance. In addition to everything else that goes on during the crisis, incident responders must consider, "What is the impact of my actions on our ability to claim against the policy?" They must ensure

that everything they do meets all of the liability coverage obligations.

There are junior-, intermediate-, and senior-level incident responders. At the most senior level, there are people who understand contracts, government regulations, and the fundamentals of insurance.

In a way, incident responders are like fortune-tellers. They understand not just the current impact but also future impact. While managing the existing situation, they must foresee where the incident's going to be in the next hour, two hours, or two days, and then try to get there before the threat actors do.

AUTOMATION EXPERT

Cyber threats are constantly evolving, and organizations that rely on manual tests to mitigate vulnerabilities quickly discover that the cyber landscape is changing so rapidly that they cannot keep up. Some companies are migrating toward automation to help manage this dynamic threat landscape. As such, cybersecurity teams need automation experts—people who can draft complex rules to automate processes.

We call this process orchestration. It involves defining exactly what steps are taken when conditions A, B, and C

happen. Compared to human-operated manual deployment, automated systems will perform these tasks much faster and with much more consistency.

Automation experts understand tools and ensure they work together seamlessly and efficiently. Such experts have very strong software development skills and are often former code developers from the application space.

DATA SCIENTIST

More and more companies are starting to look for data scientists with a specialty in security. Earlier in this chapter we talked about the SIEM tool, a giant data collection engine powered by correlation rules. Sometimes SIEMs use traditional correlation, but the newer tools are based on artificial intelligence (AI) and machine learning (ML). Security teams are now expanding their portfolio of people to include ML experts who understand algorithms and AI. They understand how to analyze massive amounts of data and generate useful information from millions of pieces of information that are ingested daily, weekly, or hourly.

Cyberattackers constantly alter their techniques and tactics, and so we never know what they're planning next. Data scientists can create filters that seek out anomalies in the environment. Then an incident responder can ask, "Is this an attack, or is this just a normal operational anomaly?"

The growing importance of data scientists illustrates one of the challenges in hiring for cybersecurity roles: skills that were important two years ago are no longer important today. Data science had no role in security two years ago, but it's becoming increasingly more important.

A good data scientist can work with any kind of data. Once retained, you will develop their cybersecurity expertise, because they have to understand what the threat actors are doing. This role is very, very difficult to fill. When you shrink the available pool of people to just security data scientists, there are even fewer. The number of people who can build good ML algorithms is miniscule; there are about a thousand in the world today.

Larger companies retain many of the available data science specialists, so there are very few left to work for other companies. This is why smaller organizations must outsource what's called "data science as a service." The best example of this is IBM's Watson, a data analytics machine-learning AI tool. The challenge with Watson is that it is prohibitively expensive for most organizations. Most small and medium-sized businesses simply can't afford it.

CHANGE MANAGER

IT security is a balancing act between security and usabil-

ity. Absolute usability means something in the system is not secure. Absolute security means that the system is not usable. Organizations strive to find a balance between the two. In most cases, the user base will be impacted and their lives will be made more difficult in exchange for heightened security. A change manager is necessary, as he/she can communicate this information and introduce the change in an inviting manner so that employee behaviour can effectively shift.

The change manager's job is to identify the stakeholders and to ask the following questions: How do we communicate to the stakeholders? How do we make the staff adopt good security behaviour? How do we get them to accept the tools that we must implement? Change management is a specialized field in general business, but when considering a change manager specifically for cybersecurity, the available pool of candidates shrinks to a very small number in any given market. These people are difficult to find and to recruit. You may have to hire a change management expert from outside the security field, or a communication expert, or a marketing expert, then develop them into the kind of security change agent that you need.

The change manager is probably the least technical role in a security team. Their skillset is an amalgamation of psychology and communication. Their specialization is

human behaviour rather than tools. Change managers understand human motivations. They understand how people will react to different stimuli, and they use this knowledge to build specific plans to change user behaviour.

COMPENSATION

Quite simply, compensation for cybersecurity roles is going up. And up. And up.

The closest example in the tech space to what's currently happening in cybersecurity is what happened to SAP fifteen years ago. There was a shortage of specialized resources, which drove up the cost of those resources. The market couldn't produce enough individuals with the right skills fast enough, and so the cost of an SAP resource doubled and tripled within a very short amount of time.

That's exactly what we're seeing in the cybersecurity space right now. Competition for skilled resources is extremely fierce. Finding qualified tools experts is difficult, not impossible. But when you start considering above that skill level, seeking to fill any of the other roles that need not only technical skills, but also people skills, ability to manage pressure, incident response, risk analysis, and so on, things get difficult. Qualified candidates are expensive, and they're getting more expensive very quickly.

Compensation is not just about salary anymore. There's extensive competition in the current hiring market on things like vacation time and other perks. We're seeing other compensation models that include company cars. I know of one company that's offering all-expense-paid annual vacations for the entire family to attract candidates.

The best approach is to treat your employees like people and think about what you would do if you genuinely cared for them. If they were a member of your family, how would you treat them? It's giving them time off. It's recognizing them. It's giving them challenges and the ability to grow and shine within the company. Everyone is different. Some want visibility. Some want increased roles and responsibilities. Some want to interact with executives and build a name for themselves. Others want to be external experts on behalf of the company. Because each employee is unique, no model works for every employee and in every situation.

What we try to do is to tailor a compensation and retention model based on each employee's needs. That is a challenge because it requires extreme effort from the leadership of the organization, security leadership, and HR. But at the current time in the current market, it's the only way.

Most CISOs don't do this, but I meet every single

employee twice a year on a one-on-one basis. Even though an employee could be removed from me by four or five positions, between all the layers of management and team leadership and directorship, I still meet them. A direct pipeline to me for every team member is a tool I use for retention.

I keep a detailed file for each employee. We talk about their hobbies, what they do outside of work, what motivates them. I also ask them what we are doing right, what we are doing wrong, and what could we do better. I ask if there is something that they would like to have that they don't have today. This information allows me to make general decisions about retention policies and strategies.

SALARY SURVEYS

It won't do any good to list salary ranges in this book because they are changing so fast. But there are some online resources that provide this data. Two organizations that issue salary reports are the ISACA (which at one time stood for Information Systems Audit and Control Association, although the organization goes by only the acronym now) and the International Information System Security Certification Consortium, (ISC)². Look up their latest salary surveys and make sure you're competitive in that range for that position.

Most medium and large organizations will have a human resources department that you can ask to perform a security salary benchmark. It's probably in your best interest to have that done every eighteen months because salaries are moving so quickly. If your salaries are lagging below industry norms, you'll begin to see your staff leaving. In some cases, when employees begin to leave, there can be a domino effect. After the first few people leave, others start asking themselves a lot of questions, and it gets them thinking, and that could start a chain reaction.

There is no way to predict how high ever-increasing cybersecurity salaries will go. But as of this writing, we've seen an increase in salary of between 20 and 50 percent in the last twenty-four to thirty-six months. There is no sign of change. As long as demand outstrips supply, prices will rise.

SKILLS MUST BE MAINTAINED

I make ongoing personal development and skills training a part of the annual performance review of every employee; it is that important. People who want to enter security need to understand that security will require—in fact, will demand—constant education and skills refinement. The pace of innovation and change is extreme. In order for me to hire an employee, the employee needs to show

an ability to learn on their own and to personally develop and grow.

I have a responsibility to help my team grow and to give them the tools they need to succeed, whether that's training material, access to a lab, on-the-job training, or working with more experienced people. The ability to learn quickly and assimilate information efficiently is a core skill that I demand from every single one of my employees, from the most junior to the most senior.

At most levels within the organization—junior, intermediary, and advanced—I strongly believe industry certifications are required, not only because they are proof of efficiency, but also because a professional certification is a marker that will bring credibility to your customers. Both ISACA and (ISC)² have multiple certification tracks. And almost every certification requires ongoing continuing education. For example, the ISACA certification for auditor, called the Certified Information Systems Auditor (CISA), requires 120 continuing education hours every three years.

I'm also a big believer in what I call education through osmosis. Pair up people of different skill levels and allow the more junior person to learn from the more senior person while on the job. They will learn the intangible skills that are highly valuable but very difficult to transfer any other way.

SECURITY STAFFING COMPANIES

One way for organizations to fill the cyber staffing gap is by buying managed services from an external cybersecurity vendor. There are, however, considerable disadvantages to outsourcing cybersecurity. First, paying an outside security consultant often costs more than hiring a full-time employee. Second, companies that outsource cybersecurity sometimes don't build the required skill-sets in-house. And third, in the worst-case scenario, I've heard of companies being held hostage by their managed service providers because their data is in the provider's control and they don't have the expertise to migrate the data or bring it back in-house.

Cybersecurity staffing companies are staffed with experienced and highly compensated consultants. Their objective is to maximize profitability by placing experts in segments or industries that are in dire need of security resources. This approach can make sense under certain situations as it provides security resources, but it comes at a premium price.

Deciding whether a staffing company is a viable option depends on many factors. For medium-sized companies, I think the organization needs to ask, "Will we need this skillset over the long term, or will we only need it for a finite period?" If the skills are not required in the long term, buying it by the hour makes sense. That way you

can bring in the resource, have the work done, and stop paying for the service once the objective is accomplished.

Small organizations that can't afford a dedicated security person will often be better served by renting a fraction of a security resource. The advantage is you're getting the services that you need with maximum flexibility, and you're not encumbered by long-term costs. The disadvantage is that the expertise doesn't belong to you, and you may not be able to access it when you need it. Plus, you'd be competing for that resource. Just as there is competition in the general market to hire employees, there is also competition for the scarce resources of a security staffing company. You're either going to pay more for that resource, or you're going to settle for a resource that's less qualified.

UNDERSTAND INDUSTRY TRENDS AND THREATS

Hiring decisions need to be informed by the changing nature of cyberattacks. One of the best resources for data and information on the cybersecurity industry as a whole is the Verizon Data Breach Investigations Report (DBIR). This annual study aggregates and analyzes information on thousands of cyberattacks around the world.

The latest Verizon DBIR examined 53,000 incidents and 2,200 data breaches from sixty-five countries. Seventy-six percent of the breaches they studied were classified as

financially motivated. Members of organized crime syndicates were behind half of all cyberattacks. Nation-state or state-affiliated actors were involved in 12 percent of the breaches. Even though state-sponsored cyberattacks get headlines in the news, they make up a relatively small percentage of total attacks. Most attacks originate from organized crime groups.

According to the current Verizon DBIR, 68 percent of the breaches that they tracked took months or longer to discover. Part of that is because people don't have the right tools. The other part of that is because organizations don't have the right employees to use those tools effectively. Effective cybersecurity builds in the tools and the expertise, the people, process, and technology to make that window between breach and detection as small as possible. So, as soon as something happens, you want to be able to quickly detect it and respond to it.

CHAPTER 5

INFORMATION SHARING AND COLLABORATION

ROBERT W. (BOB) GORDON: EXECUTIVE DIRECTOR, CCTX

Robert W. (Bob) Gordon is the executive director of the Canadian Cyber Threat Exchange (CCTX). Over his career, Bob has worked for four federal national security agencies—the Royal Canadian Mounted Police, the Canadian Security Intelligence Service, the Communications Security Establishment, and Public Safety Canada—as well as in the private sector at CGI. While serving in these roles, Bob has been a senior assistant deputy minister, led the national counterterrorism program, overseen broad technology and internal security initiatives (including personnel, IT, and physical security), and designed Canada's first Cyber Security Strategy. At the CCTX, Bob oversees information sharing and collaboration programs designed to create an open threat data exchange between the public and private sectors.

When you think about the way cyber has evolved, we've gone from tools-based countermeasures to intelligence-based countermeasures. The more intelligence you have, the more robust your defence. Having multiple points of intelligence and having a global intelligence footprint is going to be more

effective than just having a single point of observation. Sharing that intelligence makes the global community better at predicting, preventing, and responding to cyberattacks. The concept of shared intelligence, of shared brain, is extraordinarily relevant, and having more information to meet the threat is almost mandatory now. —Ajay K. Sood

There is only one internet. The government, the private sector, and the public all use it, and each party does so under the assumption that their data is secure. This fundamental trust drives the digital economy, and without it, the entire collaborative, data-driven system on which the government, the private sector, and the public have all come to depend on collapses.

In order to strengthen this system and to ensure the public's trust is well-placed, many Canadian organizations have begun taking an active role in information sharing and collaboration with other organizations—and in so doing, developing a greater awareness of the cybersecurity environment in which they operate.[5] Their approach represents a significant shift in mindset from the earlier days of e-commerce. While these organizations are committed to competing fiercely in terms of products and services, they have nevertheless embraced the idea that an even data security playing field, one in which organi-

5 The CCTX engages with businesses, government, business associations, and not-for-profit entities. The term "organization" will be used in this chapter to refer to these groups.

zations regularly collaborate and share information to better understand and protect themselves against security threats, works to everyone's mutual benefit. As such, Canadian companies need a vehicle that allows them to anonymously or with attribution share threat intelligence, whether with other individual companies, their sector, all sectors, or the nation.

In 2015, the Canadian Cyber Threat Exchange (CCTX) was founded by nine private sector companies to help facilitate these activities and to provide participating organizations with a neutral forum for sharing cyber threat information, developing best practices, and troubleshooting the many challenges of the modern cybersecurity environment.[6] The CCTX offers an ideal forum for addressing both the technical and cultural challenges associated with modern attacks, encouraging organizations to collaborate and share information not only internally, but also externally with other organizations, regardless of size, complexity, or sector. As a not-for-profit entity, the CCTX is guided by two key value propositions:

1. Act as a threat data exchange with the goal of delivering actionable intelligence to other organizations.
2. Act as a collaboration centre where cyber profession-

6 The nine founding companies of the CCTX were Air Canada, Bell Canada, Canadian National Railway Company, Hydro One Networks Inc., Manulife Financial, Royal Bank of Canada, TD Bank Group, TELUS, and TransCanada Corporation.

als from different companies can get together, talk through their issues with other professionals, and arrive at useful solutions.

These two approaches allow organizations and their security professionals to access, share, and apply information in a variety of ways, including troubleshooting isolated issues, analyzing the latest threats, and exchanging best practices, techniques, and insights.

Nine corporations started the CCTX. Today, more than thirty organizations participate from across Canada's core economic infrastructure. Participants include major telecommunications companies, five of the six major banks, five different energy companies, and major insurance and transportation companies. Such rapid expansion in just over one year's time illustrates the value of this neutral venue to Canada's data-driven economy. As more organizations participate, the CCTX has been able to focus its membership drive beyond the traditional core infrastructure and into sectors such as retail, professional services, entertainment, and technology. Even smaller organizations have begun joining the fold, with the CCTX enhancing its offerings to suit the needs of all its members.

Through the CCTX, both the private sector and the Canadian government are empowered to collaborate and share threat information and technical capabilities with unprec-

edented transparency. This chapter explores the role of this shared space and how it came to be, the benefits to participating organizations, and how the CCTX model is facilitating a new kind of relationship between the public and the private sectors.

THE BENEFIT OF SHARING AND COLLABORATION

When considering information sharing and collaboration, most organizations begin with a simple question: why? Working in a spirit of mutual assistance might sound feasible in a broad, philosophical sense, but organizations are eager to understand the benefits such a program might provide them and why they should participate. Perhaps the greatest benefit to organizations is that their participation helps strengthen the Canadian economy and infrastructure. However, other benefits to individual organizations abound as well.

First, information sharing gives participating organizations access to more data—and more data means better intelligence. By sharing information, organizations can add to the data they've already collected from internal monitoring systems and make it more actionable, enabling them to better protect against attackers infiltrating their network and to more quickly identify attackers already in their system.

Second, information sharing and collaboration allows

organizations to leverage the knowledge of others. Speaking generally, attackers will use the same approaches over and over again until they don't work anymore. By sharing information, organizations are able to shorten the lifespan of an attack product, forcing the attacker to spend more resources developing new attacks. The more time and money those attackers are spending developing new attacks, the less time they're spending attacking individual organizations.

Third, participation in a collaboration centre offers a cost-effective intelligence solution. Information sharing means organizations don't have to protect themselves entirely on their own. Collaboration centres typically have cyber analysts on staff to analyze data and develop effective defences for other organizations to use. In a country like Canada, where 99.7 percent of businesses are classified as small or medium, most organizations can't collect, analyze, and defend all on their own.[7] By participating in a collaboration centre, these businesses benefit from extra protection at a fraction of the cost.

A fourth benefit is the protection collaboration offers to organizations' clients and vendors. Many businesses require clients, customers, or vendors to connect to their network, whether to place orders, send or receive infor-

7 "Key Small Business Statistics—June 2016," Government of Canada, November 11, 2016, https://www.ic.gc.ca/eic/site/061.nsf/eng/h_03018.html#point1-1

mation, or access data in some other way. While these businesses naturally depend on this external access, a network is only as strong as its most vulnerable user.

For example, in one recent attack, a company was breached through its HVAC system, which was connected both to its network and to its third-party air conditioning vendor. Because that vendor was vulnerable to attack, so was the company. By collaborating and sharing information, not only do organizations better protect themselves, but they also better protect their clients and vendors, thereby reducing the likelihood of an interruption in service or a break in the supply chain.

Recent research bears this out. For instance, in the 2016 report "Flipping the Economics of Attacks," written by the Ponemon Institute, researchers found that an average of 39 percent of all hacks to Canadian companies can be prevented by organizations sharing threat intelligence with their peers.[8] When viewed in this light, it becomes clear that sharing threat intelligence is not merely a good idea, but one of the most effective strategies an organization can take to prevent attacks.

Finally, participation helps organizations better identify

8 Ponemon Institute, "Flipping the Economics of Attacks," Palo Alto Networks, January 2016, 3, https://www.paloaltonetworks.com/content/dam/creative-assets/campaigns/corporate/ponemon-report/web-assets/PAN_Ponemon_Report.pdf

indicators of compromise. Once an attacker has breached a network, their goal is to learn as much as they can about that network—how it works, what data is most important, and how they can exfiltrate it. Attackers often spend weeks or months to uncover this information, with a mean "dwell time" of 191 days. During this period, most organizations are unaware they've been compromised.[9]

Identifying indicators of compromise is no easy task. While companies are constantly monitoring their networks to find evidence of an attack, such an effort can amount to searching for a needle in a haystack. Even with an advanced combination of software and hardware, an attacker could lay undetected for a considerable period of time.

Through a collaboration centre, when one organization ultimately finds an indicator of compromise, they can share that information, and in so doing, improve other organizations' detection capabilities. When enough organizations share enough of these indicators, that giant haystack becomes much smaller, leaving attackers with fewer places to hide, dramatically reducing their dwell time, and decreasing the likelihood they will uncover any information of value.

9 Ponemon Institute, "2017 Cost of Data Breach Study," IBM Security, June 2017, 2, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130CAEN

RESPONDING TO A CHANGING LANDSCAPE

Another factor driving organizations to participate in an information exchange is the changing cybersecurity landscape. Two different factors have contributed to the current climate. The first is a shift in attacker behaviour. Where formerly attackers would focus on organizations in a particular industry, they eventually realized the industry type didn't matter; their ransomware or malware would work just as easily against a retailer as it would against a hospital or an airport. As long as the hacker could find a way to profit from the attack, the target itself didn't matter.

At the same time, a second factor came into play: businesses began diversifying. E-commerce is everywhere. Retailers now run financial components of their business, telecommunications companies have ventured into retail, and hydroelectric companies have expanded into internet services. While diversification may be good for business, it also increases the number of potential exposures.

These converging trends ultimately gave rise to the CCTX in 2015. As the nature and frequency of attacks became more sophisticated, Canadian businesses began to realize that information sharing and collaboration with other organizations would allow them to adapt more quickly in a constantly changing cybersecurity environment. As the CCTX began to take shape, the question was: How

would they do it? What would they build, how would it be structured, and how would it be funded?

The first goal of the CCTX was deciding on an approach that accounted for all sectors of the economy. The traditional approach to critical infrastructure protection focused on the three crucial sectors of Canada's information infrastructure: telecommunications, energy, and finance. If any one of those sectors went down, the consequences would ripple out into the rest of the economy.

While these sectors made for a good starting point, the CCTX knew that in the digital, internet-connected era, such a narrow focus would be inadequate over the long term. The new data economy is structured in a way that allows any organization producing intellectual property to share its data with other parties—and attackers know this. Rather than go to the originators of the data, who are usually large organizations likely to spend considerable resources on cyber defence, attackers find entry points that aren't as well-guarded, such as the supply-chain organizations that might do business with these larger firms. These intersections of data, personal information, and intellectual property affect all sectors of the economy, accounting for the many daily interactions between the small, midsize, and large businesses and clients that make up the supply chain.

THE EVOLUTION OF ATTACKS

As attackers began to expand across industries, the nature of those attacks evolved as well. Whereas in previous decades, attacks often amounted to data theft, modern attacks include denial of service, ransomware, and more recently, destruction.

Whatever the case, one of the main goals of the CCTX is to help organizations understand the nature of these threats and how they can ensure their data is secure. With this understanding comes an effort by organizations to produce both technical and business solutions that address two basic cybersecurity considerations:

1. What data are of value to the organization?
2. Where is that data stored, and who has access to it?

When considering the different kinds of attacks a modern organization likely will face, these questions become essential in developing a comprehensive cybersecurity strategy.

WHOSE DATA SHOULD BE PROTECTED?

Many organizations don't think they have the sort of data or intellectual property that hackers want to steal. Unfortunately, such a perfect, invulnerable organization doesn't exist. Every organization has data that make up their

point of difference or their business value. Whatever this information is, hackers want it—and once they find it, they will either steal it or deny the organization access to it.

As a simple example, consider the personal family photographs many people store on their computers or in the cloud. As long as those data have value to the owner, an attacker is incentivized to steal them and demand, say, one hundred dollars for their safe return. Suddenly, the owner is left in a precarious position: do they pay the ransom, or do they sacrifice a potential lifetime of personal memories? Businesses often find themselves in the same situation; they don't know they have anything valuable until it has been stolen or held for ransom. At that point, they're either forced to pay to get it back or find some other way to limit the damage such a breach might have caused.

CREATING A PROACTIVE CYBERSECURITY CULTURE

Another challenge businesses face is determining whether they've been attacked. While it's easy to assume that such responsibility falls purely in the hands of IT, in reality, these efforts require a transparent culture that involves every employee. For instance, while an organization may have a policy to never pay a ransomware attack, an embarrassed employee interested in keeping their job or meeting a deadline might react differently and pay a ransom out of their own pocket.

For this reason, organizations must be proactive in creating a positive culture relative to cybersecurity that encourages employees to report an attack, rather than penalizing them. Otherwise, one of two things could happen:

1. The embarrassed employee might pay the ransom, and nothing happens. The attacker simply holds onto the data, perhaps demanding additional ransom.
2. The employee regains access to their data, but the attack software is still in their system. A month down the road, the attacker comes back and holds the data for ransom again.

If an employee struggles with this attacker in secret, the organization remains unaware of the problem until it interrupts day-to-day business, perhaps shutting down access to key information at a crucial point in a major deal.

Adding to this challenge is the decentralized nature of modern business. In the modern world, corporate information no longer resides in a single secure computer centre. Corporate networks are now diffuse: employees use a combination of laptops, smartphones, and tablets to access the organization's data on any given day. Each one of those devices offers attackers a potential window into an organization's data.

To protect themselves, companies must always ensure

they know what their sensitive data is, where it is stored, who has access to it, and what regimes they have in place to respond to an incoming attack. Business units, not just the IT group, need to be involved in this analysis, as only they can assess the value of the information and the impact on business operations if that data becomes unreliable or unavailable. Just as important, however, they must set an internal environment that encourages employees to have confidence in the system and report any problems immediately as they occur. A neutral, collaborative organization can be an invaluable resource in meeting those ends.

THE THREAT DATA EXCHANGE

The CCTX collects its data, which it then melds into a comprehensive, actionable dataset, from three broad sources. The first is member organizations. Their data can be submitted as unstructured data manually entered into the CCTX portal or in a structured format, which is readily machine-readable. Two separate processes, which are referred to as "STIX and TAXII,"[10] enable organizations to characterize their data and ship it electronically with minimal human intervention. The data provided by participating companies are anonymized, meaning no piece of information is attributed to a specific organization.

10 These acronyms stand for Structured Threat Information eXpression™ and Trusted Automated eXchange of Indicator Information™, respectively.

The second source of data is the Canadian federal government, which offers a few unique capabilities. For example, one of the resources provided by the Canadian Cyber Incident Response Centre (CCIRC) is their database on malware and threat analysis, which offers a vital resource for the private sector and the CCTX's efforts. Recently, the Canadian government announced it would be creating a new Canadian Centre for Cyber Security, which will bring together capabilities from the CCIRC and the Cyber Operations Centre in Shared Services Canada and the IT Security component in the Communications Security Establishment. The capabilities and information collected from these sources will then go out as a single source of information to the private sector to help protect the core critical infrastructure.

The third source from which the CCTX will obtain cyber threat information is commercial threat services. In the interest of gathering more robust data, the CCTX has plans to begin buying commercial sources of threat data from commercial service providers.

The CCTX then aggregates and analyzes the data from these three sources to create a variety of reports, whether for tactical decision-making in the moment of an attack or for more strategic long-term business decision-making. These reports will be tailored so organizations of varying sizes can absorb the information and thereby understand

both internal and external threats and how they might affect their business. Through this positive exchange with the private sector and the government, the CCTX is able to contextualize knowledge from a variety of sources and use that information to participants' mutual benefit.

THE COLLABORATION CENTRE

Organizations investing in cybersecurity analytics and services often do so with a healthy dose of skepticism, a suspicion that they don't actually need whatever they're being sold. Information-sharing groups such as the CCTX, however, are neutral. They don't represent any products or services. They seek only to share data in an open exchange as a means of empowering organizations to make more informed security decisions and create a more secure infrastructure to bolster the Canadian economy.

At CCTX, businesses can meet on equal ground with those who would normally be considered competitors, suppliers, or customers, and in the process, gain a deeper understanding of the security issues facing all sectors of the Canadian economy. Through this ongoing exchange, these organizations are better equipped to assess risk, adopt new tools and processes, and make better strategic decisions.

As these tools and processes develop, small to midsize

businesses particularly stand to gain from the resources offered by the collaboration centre. While larger organizations may have more robust capabilities when it comes to big data analytics and assessing potential threats, the majority of organizations do not. To better assist all sizes of participating businesses, the collaboration centre provides services in three areas: communities of interest, communities of trust, and an on-site collaboration facility.

1. COMMUNITIES OF INTEREST

This capability provides opportunities for cyber professionals to collaborate and mitigate current cybersecurity threats. Activities include whiteboard sessions, conference calls, and discussions with thought leaders from the private sector who share their thoughts on trending topics such as ransomware, supervisory control and data acquisition (SCADA) systems, data loss prevention, and insider threats.

2. COMMUNITIES OF TRUST

This capability allows organizations to come together in smaller groups to exchange information or discuss ideas that are either too sensitive to address broadly or too specific to impact most other businesses. Secure, segmented compartments within the CCTX portal have been established where organizations can share information

traditionally considered too sensitive for sharing with other organizations. Although the details of exchanges will remain solely among those organizations providing the information, the general results will be shared among the broader membership.

3. ON-SITE ANALYSIS

Through this hands-on offering at the collaboration centre, organizations can send their analysts in to work out issues side-by-side. As a neutral ground, the CCTX's collaboration centre is an ideal environment for such efforts, allowing organizations to share specific information, but in a limited context so they don't disclose any corporate sensitive information.

BUILDING TRUST

The most interesting element to come out of the CCTX's collaboration and information-sharing program is the way in which it has built trust within the private sector. A primary goal of the CCTX has been to acclimate cyber analysts to the idea that they could sit down and exchange ideas with other professionals—even those in competing organizations—and discuss topics of mutual interest, emerging technologies, interesting findings, and best practices surrounding recent attacks. Through this process, participating organizations and analysts have found the following:

- Even competing organizations can work together in their industry's mutual interest.
- Organizations are encouraging their professionals to participate and are excited about the return on investment to the organization.
- Professionals are seeing clear value from their conversations, emerging with more knowledge and a better understanding of their problems and potential solutions.

Many organizations choose to participate in collaboration centres as a means of exercising leadership in the cybersecurity community. While that opportunity is always available, participants are often surprised by how much they learn from others rather than by how much they share. They see firsthand the value of the threat data exchange or the collaboration centre as a means of learning more about pressing issues and emerging with actionable solutions.

Through their participation, collaboration, and thought leadership, organizations often discover new business opportunities—whether to provide solutions to new clients or to find new vendors they can trust. When a vendor company comes to the collaboration centre and discusses current trends, participants sitting in on the talk might realize a pressing need in a specific area and see the vendor company as well-equipped to offer a solution.

AN ECONOMIC LEADER IN CYBERSECURITY

The initial success of the CCTX has far-reaching positive implications for the Canadian economy, where data is now the new digital currency. Already a world leader in privacy legislation, Canada now has a model for information sharing and collaboration that is attracting increased attention from the global cybersecurity community.

Through these efforts, the CCTX is helping to reframe the conversation surrounding cybersecurity from one of cost to one of opportunity. Not only is Canada host to a wide variety of established and startup organizations with cutting-edge cybersecurity products and services, it also has an engaged private-sector community to ensure continued thought leadership in this area.

Through its proactive policies and legal environment, Canada has begun to realize the tremendous economic opportunity in the world of cybersecurity. To continue to establish Canadian businesses as the go-to solutions for secure data storage, manipulation, technology, and analytics, collaborative organizations must continue to provide an open forum for their participants to learn, innovate, and continue to build a competitive advantage in the industry.

Working in collaboration, we can create a more cyber-resilient Canada—where businesses focus on delivering

goods and services, where individuals derive benefit from a digital world knowing their privacy and security are protected, and where Canada's economic prosperity continues to expand. No one can do this alone. This vision is achievable. The CCTX is building a community that is delivering that vision. The opportunity is now for organizations of all sizes, from all sectors, to be part of this collaborative community.

CHAPTER 6

MOVING FROM WATERFALL TO DEVOPS FRAMEWORKS

VIVEK KHINDRIA: HEAD OF CYBER AND INFORMATION SECURITY, BELL CANADA

Vivek Khindria has over fifteen years' experience in North American financial institution technology and cybersecurity, and over five years in telecommunications cybersecurity. He is the elected representative for Canada on the executive council for Information Security Forum, a global Fortune 500 member-driven organization focused on security practices, tools, and research. Since 2016, Vivek has been the secretary of the Canadian Cyber Threat Exchange (CCTX), an organization that supports the sharing, analytics, and collaboration of cyber threat information across sectors and with other sharing hubs to help protect Canadian businesses, governments, and consumers to strengthen Canada's economic prosperity.

We've had to take a long look at ourselves in the software development community and redefine the way we develop software for the enterprise and for the world. Cybersecurity now has become something that must be built in from the start, as opposed to bolted on after the fact. We can no

longer just put a security wrapper around software systems and processes and expect them to be safe. Security has to be designed in from the very beginning, into everything we build and code. Changing the way we write code and changing the way we test code is what this chapter is about. —Ajay K. Sood

In most industries, key processes and methods will all evolve over time. A process that worked twenty years ago may begin to show its age, and new methods will come along that are better suited to current conditions in the marketplace, including the mindsets of the scarce workforce we are all competing for. This is the case with enterprise-software development methodologies. The intense competition in software development resources, especially with security competencies, has pushed organizations to adopt the best and most effective methods for coordinating teams of developers to create software that users want as fast as possible, but not always with security in mind. Today there is a transition taking place from waterfall to agile and DevOps. Bell Canada is about four years into this transition, and it is a massive transformation. Let's take a closer look at these methodologies and why change is happening.

WATERFALL, AGILE, AND DEVOPS

Most professionals who work in software development are familiar with the basics of waterfall, agile, and DevOps

methodologies. The waterfall development model has been around since the 1970s and typically involves the following steps: First, agree upon and define the precise requirements. Second, create a design to meet those agreed upon requirements. Third, build the full product over a period of months. Fourth, once it's built, the developers test the product. Fifth, after testing it, they deliver it to the end user or customer, have them deploy the application, and get them to sign off on it and go live. When users begin using the product and bugs or issues arise, the development team makes plans to address them, spawning new waterfall initiatives in some cases, depending on how big a change is required to fix the issue—but either way, the cycle starts over again to retest, deploy, and go live.

Waterfall methodology is a sequential process that got its name because it flows in a downward progression, like a stream flowing downhill or down a flowchart. All of these steps are done in order; each one begins after the completion of the previous step. It makes sense, and for decades, this was the method by which most developers created enterprise software. Many organizations continue this practice today. There are many reasons for the inertia, including resistance to change, governance processes tuned to waterfall, financial processes tuned to waterfall, and procurement processes tuned to waterfall. One advantage of waterfall methodology is that it is a

highly formalized and tightly controlled development process that begins with careful planning and ends with a finished product that perfectly meets the requirements stated at the outset, but that does not mean the resulting product is the right thing at the right time.

DISADVANTAGES OF WATERFALL

The big disadvantage of waterfall is that doing all these steps in order takes a lot of time. When development teams build applications using the waterfall methodology, the project duration is measured in months or fiscal quarters. A project may take six, twelve, or eighteen months to complete. Highly complex software systems could take several years. Feedback occurs primarily near the end of the development cycle when the end user begins to look at the product.

During that eighteen-month development process, the business world changes. Competition changes. Security vulnerabilities change. Threats change. New technologies and cloud services become available. Waterfall is a serial, systematic, slow, and methodical process. Internet speeds drive the need for change at a pace that is too fast for waterfall to keep up.

Nevertheless, in the world of cybersecurity, many companies' assurance methodologies and frameworks still

are geared around waterfall. Despite the considerable disadvantages, waterfall still is the dominant methodology, but its dominance is shrinking every day.

ADVANTAGES OF AGILE AND DEVOPS

In contrast, the agile methodology moves fast. Agile is a methodology built around small development efforts called sprints. Companies developing with agile may have sprints that last anywhere from a few days to a few weeks. The goal is to rapidly develop a "minimum viable product" (MVP) that is functional enough for the end user to start using, even though there may be some bugs or missing features. The idea is to build fast, do some minimal testing, go live by getting the product into the hands of users, test it on the fly more thoroughly, collect feedback, refine, and repeat the process every few weeks. In agile, the development, use, testing, and bug fixing happen in parallel. The minimum viable product is derived by the scrum master (also called the sprint leader) and dialogue with the sprint team from the collection of stories used to describe the elements of the product being developed.

The big advantage of the agile methodology is agility and speed; there is no need to wait patiently for months or a year before you can start using something you want now. If a bug is discovered, it can be fixed in the next release. Each new feature or fix feeds into the next release.

Companies like Google and Facebook often issue new releases every day!

This is why we're seeing a rapid adoption of agile across the security industry. Companies often don't really know at the outset what they need to build. Agile allows them to find their way, iterating as they go. It also forces you to prioritize on the key stories so that you can hit the ground running sooner rather than later.

DevOps began in 2007 in Belgium, and it is the latest evolution of the agile methodology, although some people consider DevOps to be more of a culture than a methodology. DevOps is a way of organizing and combining two different functions—development and operations—that were traditionally kept on separate teams. In the past, the development team typically would work in one office while operations worked in a different office. There would literally—and figuratively—be a wall between them. Because developers don't want to do operations, and the operations team doesn't have the skills to do development, there is little overlap. This is sometimes referred to as the wall of confusion because development and operations don't always understand each other. The two teams communicate when necessary but are largely separate entities with different skills and objectives. In this segregation of duty, poor software development can impact the operations team, and poor

operations can lead to more demands on the software development team.

DevOps tears down that dividing wall. DevOps is a culture built on the realization that combining those two different functions into one team with shared objectives, often in the same office, has tremendous benefits. In DevOps, the development team and the operations team work hand in glove. That's where the magic happens. When the two work together as one, often literally side by side, great synergies and clarity of issues can occur. This is one of the key benefits of DevOps.

SOME PITFALLS TO MANAGE WHEN USING AGILE AND DEVOPS

There are some pitfalls one can face when adopting agile and DevOps. These mostly centre around the rapid pace at which these methodologies move. For example, when a DevOps team is issuing new releases every couple of weeks, or even every couple of days, proper documentation of each release can become an afterthought. This includes all of the traditional disciplines like asset management, change management, incident management, and security testing.

These fast-moving methodologies are not an excuse to not document. DevOps is not an excuse to take shortcuts

in security. Proper documentation and sourcing are still essential and critical, especially in an internet-facing world. But in the excitement of the sprint and the race to the next release, some of these crucial risk-management and incident-prevention steps can be missed.

Another potential pitfall when you have teams building fast on the fly occurs when they incorporate open source code without tracking each source code segment as an asset. The code leveraged may have unique licensing requirements and it may also have inherent bugs, some of which we know today and some of which we will learn about tomorrow. These risks need to be managed carefully, otherwise it can create asset-management nightmares down the line.

The concept of shared code is not new, but in the context of DevOps and agile there is a dimension around automation, virtualization, APIs, and standard protocols so that the whole environment is built and deployed with open-stack and orchestration protocols. This environment should be tuned and monitored through different kinds of automation, leading right to the security monitoring on the security operations centre (SOC) side. Security isn't an option; it should be built right into the whole deployment mechanism for those virtualized components.

SECURITY IN DEVOPS/AGILE

Testing throughout the agile process is essential but complicated, as there are so many different types of testing. There is syntax testing, integration testing at the code level, regression testing, capacity testing, performance testing, user acceptance testing, exception testing, and penetration testing. Security scans of the source code and vulnerability scans of the applications and systems are now part of many software development life cycles (SDLC). Running dynamic code analysis tools that look specifically at application vulnerabilities while the program is running has become another valuable insight into the security and memory efficiency of the applications.

All of this testing can be and feel like a huge overhead. An agile/DevOps team working on a two-week sprint might not appear to be able to squeeze all these tests in. The key is to automate where you can and to build a pipeline so the right test cases accumulate in the library and the test teams can access them as appropriate and relevant.

A key challenge in agile is that every team cannot always have a full-time security expert in their sprint. In a few special cases, a team may actually get a security expert on their project, but it's rare, because these resources are hard to find and retain. For the vast majority of projects, everyone must step up and understand that security is part of everyone's job. This is done through security training,

awareness and understanding of the risks, mentoring, tools, clear policies, standards, procedures, peer-to-peer coaching, and peer-to-peer code review.

Organizations must develop key performance indicators (KPIs) and a dashboard or scorecard to track security measures and performance objectives and drive the right behaviours and accountabilities. This also requires setting a security baseline. One way to accelerate the various teams is to build a shared base set of security capabilities and a set of code objects that the teams can draw from. You want your teams to learn and innovate on code, but not always on security sections of code: authentication, handling digital certificates, or handling password resets, as examples. We can define a number of specific categories of security services that individual developers should leverage. This can be a challenge to the whole agile mindset, which is one of empowering people and allowing them to innovate, but not necessarily on foundational components like security or protocol stacks, or well-established open standards.

THE ROLE OF THE SECURITY OPERATIONS CENTRE (SOC)

There is a large supply of cyber threat intelligence available to organizations today—far more than has been available in years past. Every vendor, every product, every intelligence organization is creating threat intelligence

and making it available to customers and vendors. Of course, there are varying degrees of quality, actionability, and context. So what, then, is the purpose of the SOC?

One of the key roles for the SOC is, in being the first line of defence, to monitor security events of critical systems; to identify and prioritize potential threats; and to respond when appropriate to contain, secure, and preserve evidence to ensure service is restored in a secure manner. The second key role is to proactively validate good cyber hygiene to prevent unwanted events from occurring in the first place.

In my model of the SOC, there are threat analysts conducting research and testing systems who sit outside that SOC, but who interact very closely with the SOC, even co-located where possible. The businesses and the customers obviously should feel the presence of the SOC via dashboards, notifications, and follow-ups, demonstrating on a continuous basis that the SOC is working to protect them 24/7.

Working in the SOC is a tough job. Being on the front lines every day means digging through the volume of alerts, prioritizing, and discarding false positives. The staff is overloaded with alerts. There are many false positives. The hours include shift work and overnights. That's why most organizations tend to staff the SOC front line Level

1 security analysts with junior people. A Level 1 security analyst in the SOC is an entry-level position to many security career ladders. As soon as someone who works in the SOC has some security experience, they look to move on to other roles, either in the SOC or elsewhere in security.

This creates a risk for organizations. Our most junior resources are on the front line of the SOC following scripts and procedures while possessing the lowest level of experience. Turnover may also be highest in this role as compared to other security posts.

THE FUTURE OF THE SOC DEPENDS ON DATA ANALYTICS AND MACHINE LEARNING

One solution to the SOC challenge is big data analytics platforms. The most famous one in a security context is IBM's Watson. This powerful but very expensive tool can help SOCs analyze data to identify and assess potential threats. Most of the correlation platforms have started moving toward this direction, from simple pattern-matching rules to machine-learning algorithms. Big companies and big governments have been building their own big data platforms for some time. At Bell Canada, we've built our own security big data analytics platform. The platform analyzes an event that our SOC sees by applying higher-order learning to pattern recognition and detections. It allows us to create threat intelligence that

is high quality, with context, and actionable—whether it's for our own systems or for customers for whom we're providing managed security services.

The big data analytics space continues to evolve both mathematical correlation models and machine learning models in both supervised and unsupervised cases. These latter examples are also referred to as artificial intelligence (AI). AI systems are capable of learning with or without any training data and can learn how certain patterns or indicators of malicious activity can be identified for action. This really represents the next frontier for a highly responsive defence capability operating at the speeds with which cyber threats attack.

The SOCs of the future are going to rely heavily on big data analytics platforms and artificial intelligence using machine learning. These systems will still require external cyber threat intelligence sources. No single company can see it all, not even a company running a massive national infrastructure. Enterprises will either have the big data platform in-house, where they consume the intelligence about internal events or, if they're not big enough to have their own platform or possess insufficient data to correlate against, they'll subscribe to platforms and security supplier clouds that mix their data with other organizations to achieve the critical mass required. Many security technology providers have built this capability into their

products, enabling the pain from one customer to be shared and leveraged across other customers using the same product. Getting this cyber threat intelligence to flow across different product groups is where it becomes more difficult, despite security-data schema standards like STIX/TAXII. Groups of companies may also try to share a common SOC, which can have the added benefit of then being able to collect and share threat data across multiple companies and attacks.

In the future, automation and artificial intelligence will be available to tens of thousands of smaller companies, potentially as small as those with just one IT employee. In the future, they will most likely not have servers in their flower shop or retail store; all their data will be in the cloud and back in the data centre, where everything is securely monitored by a group that has those machine-learning algorithms. That small company can then have a service that will proactively analyze potential threats and react quickly, but also predict where attacks will likely come from.

It's also likely that the SOCs of the future will be more directly connected with government entities because governments will play a greater role in cyber protection. In Canada we already have the Canadian Cyber Incident Response Centre (CCIRC) and the Canadian Cyber Threat Exchange (CCTX). Other countries have or are forming

similar groups to help protect their industries, citizens, and economies.

In today's world, the following scenario is completely possible: A search engine scrapes the web, including Reddit, Pastebin, and the dark web, and determines that there's a discussion going on regarding the vulnerabilities of Company XYZ. Having detected that, the SOC sends an alert to Company XYZ. The company's systems validate the vulnerability that's being cross-referenced, identifying which systems are vulnerable and which systems might not be vulnerable. They initiate remediation and countermeasures to protect that vulnerability and layer on additional defences and monitoring for a period of time. Here SOCs should count the attempts now being thwarted, which we refer to as risky events of negligible impact (RENIs).

All of that can happen in a fully automated context, today, without human involvement. That execution is getting faster and faster. The faster an organization can identify an attack and implement countermeasures, the less data will be breached, if any. Eventually all of those steps I mentioned above will happen in a matter of milliseconds, not weeks or months. People are not fully comfortable yet in automating security defences to that degree. The scars of the overload of false positives from massive SIEM deployments showed we were not ready to fully automate

the actions without substantial investments in tuning. But we are getting closer to that level of confidence more and more each day.

NOC VERSUS SOC

Many enterprise companies keep the network operations centre (NOC) separate from the security operations centre (SOC). But those two need to converge. The benefits of combining these two centres are substantial.

The difference between a server that's simply overloaded and a server that's under attack can be very subtle in some cases. Often you can be dealing with both at the same time. This discussion is an illustration of the concept that security is everyone's job, for security really is embedded in the NOC's job description, not just the SOC's. The security industry created the SOC to separate different skillsets, segregate duties, support governance, and support oversight, but the best synergy lies in combining the two.

I believe the NOC and the SOC will converge into one. They have to, because one team should have the skills to do first-level triage. Many successful companies already are integrating those functions, or at least locating the NOC and SOC in the same building. Some of the best SOC analysts are people who once worked in the NOC.

In the future, organizations are still going to need security specialists, but they're not going to need a specialist to do first-level triage; the NOC—or a renamed, combined entity that supplants it—is going to do that triage. This goes back to security being everyone's job, including the NOC.

SECURITY IS EVERYONE'S JOB

A company's success in managing cybersecurity threats is going to depend on having the right information to support risk decisions and having everyone understand how cyber threats apply to their job. Whether it's the receptionist who just got an email saying a UPS package has arrived so "click here," or a database programmer, or a systems administrator, or a procurement officer, or a business leader—everyone has to be vigilant and educate themselves on cyber threats. They must understand that their job is part of that protection, detection, and response fabric.

The most secure companies have everyone knowing and playing a role in their cyber defence system. Maybe it's alerting the security operations centre or a manager of a potential breach. Maybe it's holding suppliers and manufacturers accountable for securing data on their end. Perhaps it's having a willingness to share and contribute. Or it could be a willingness simply to not take those

shortcuts that create vulnerabilities that the threat actors could exploit.

SECURITY ACCOUNTABILITIES SAY A LOT

I can tell a lot about an organization simply by how they treat security accountabilities. If the company confines their security efforts to a single department or person, I worry. But if an organization mandates that security functions everywhere and with every person, and they train all their employees on security, I can tell they get it and may actually have a chance.

I'm lucky that I work for a very forward-thinking company that is tremendously conscious of the security threats we face in the world today. Bell Canada is a huge retail and media giant with operations in telephone, satellite, internet, and data centres. Those are all big sectors that criminals love to attack, so we have to defend them vigorously. Fortunately, we get to learn how best to do it and we get lots of data from the practice of doing so.

It's our national responsibility to leverage that data for good, to create services that are affordable, to contribute to groups like CCTX, and to share cyber threat information and intelligence. I envision Canada soon getting to a point where it's not only the most online country in the world, it's not only the most trusted country in the world,

but it's also the most cyber-resilient country in the world. We are already heading in that direction. IoT and 5G will further test and challenge us in the security space.

The economic advantage for the attacker is approximately 400 to 1. We have to get on average 400 things right on every cyber-exposed system. The hacker only has to find one vulnerability. Security by design, security baked in from the start, and systems that fail in secure ways all change the 400 to 1 ratio.

CLOSING THOUGHTS TO REMEMBER

- Trust but verify. Zero-trust systems cannot assume anything.
- Know thy enemy, his motivation, and methods.
- Defence in depth. There are no silver bullets.
- Assume the hacker is on the inside; so how would you quickly detect and contain them?

CHAPTER 7

YOU CAN'T PROTECT THE UNKNOWN: ESTABLISHING AND MAINTAINING VISIBILITY

DOLEV FARHI: LEAD SECURITY ENGINEER, PAYTM LABS/ FOUNDER, DEFCON 416

Dolev Farhi is an information security engineer who specializes in Linux/UNIX security, web application security, and offensive security. Since starting his security career eight years ago, he has worked for several security firms, including CyberArk and F5 Networks, and provided training for official Linux certification tracks. He is currently employed by Paytm Labs, which builds technologies that power Paytm, the world's fastest-growing mobile payment and commerce ecosystem. Dolev is a founder of DEFCON Toronto, a popular Toronto-based hacker group. He holds several industry-recognized certifications, such as CISSP, RHCE, and LPIC-3. He also manages the largest Linux infrastructure and security community forum in Israel. In his spare time, he builds Capture the Flag challenges for DEFCON Toronto.

The biggest thing you need to accept as a cyber professional is the inevitability of failure. Truly embracing and accepting that inevitability is part of the job. You can't protect what

you don't understand, you can't guard against what hasn't occurred yet. This is an important paradox in cyber; you're coding a defence that has to be ready for every eventuality, which is highly complex. In contrast, hackers are coding an offence; they see a hole, a way through, and they devise a tool to exploit that vulnerability. Coding an offence is a lot easier than coding a defence. In cybersecurity, we need to code a defence with the added layer of the inevitability of failure wrapped around it. —Ajay K. Sood

To understand your responsibilities as a security team, you must have a clear view of the data within the company. Below are a few questions any security team must be able to answer:

- What data do we have?
- Where is the data stored?
- How sensitive is the data?
- Who has access to the data?
- How often is the data accessed?
- How is the data stored?
- How long should the data be stored for?
- How should the data be erased?

The more you understand what is in your network, the better prepared you will be to address security gaps and vulnerabilities.

Up to now, many companies have applied a traditional approach to security in order to protect their data. This approach trusts everything within the company's known network and infrastructure. In this chapter, we will consider a new methodology for addressing security concerns in the corporate environment, an approach that establishes and maintains visibility at all times.

FROM TRUST-BUT-VERIFY TO ZERO TRUST

The traditional trust-but-verify approach to security, also known as "perimeter security," uses a logical "wall" that isolates an internal network from the internet. With this approach, companies have generally considered anything coming from the internet as unsafe. Links, emails with attachments, downloads, sketchy websites, traffic originating from some parts of the world, and even websites with certain keywords are all potential threats to the company. On the other hand, everything inside the company's internal network—as long as it has been verified once—is trusted and considered safe. From the attacker's perspective, once this protective wall is breached, the countdown to an exploit begins.

The wall between the company and the internet is usually a firewall or another network device that filters traffic travelling in and out of the company's perimeter. Sometimes the filter uses a basic rule, such as "Allow all outgoing

traffic, but reject anything that comes in." In more optimistic scenarios, a company will use a smart firewall with advanced security capabilities and a more restrictive firewall policy. Whatever the case might be, the problem remains: if someone gets past that wall, whether or not they have malicious intent, they are considered trusted and now have access to the entire network, just like any legitimate user. In a best-case scenario, the network is segregated so that an attacker can only access a specific network, which should prevent access to other, more sensitive networks.

One problem with the trust-but-verify approach is that companies rarely treat their internal resources like they would treat a publicly facing asset. Servers are unpatched, networks are free for all, and passwords are rarely rotated. If you have ever deployed a publicly facing server, you know it requires special care: proper configuration, hardening, IP whitelisting for access, monitoring, and more. There are obvious reasons for such special care. The server is exposed to the world and can potentially be targeted. Now consider how you might deploy an internal server in your company. Were the same countermeasures applied to the internal server as the external one? If the answer is yes, you are unique compared to the average company.

The second major problem with trust-but-verify is the assumption that everything inside the internal network is

safe to begin with. To understand how internal networks function, think of your simple home network. At home, you typically have a router, which protects your internal network from the internet. By default, routers discard incoming traffic and allow outgoing traffic. In some cases, you may need to expose an internal service to the internet for remote access. You could remotely connect using a home storage device, such as network attached storage (NAS). In this case, you will likely need to explicitly configure your router to allow inbound connections to your NAS.

Similar to your home network, most companies have a large internal network with many connected devices—laptops, desktops, printers, servers, storage devices, and more. With a trust-but-verify approach, all of the above are considered trusted. These days, a company's cloud environments are also connected directly to the company's network, to make it easier for employees to access cloud-based resources. Whether the company leverages cloud technologies or hosts its own servers, both are considered trusted networks.

At first glance, this traditional approach to security might seem sufficient. However, when you peel back the layers, you realize that it only takes one step for determined attackers to get into your network. And once they are in, it will be difficult to detect and mitigate the breach without a mature, security-aware environment. Reports show that attacks often go unnoticed for months, if not years.

WHY "VERIFYING" ISN'T ENOUGH

Consider your home network once more. If you need to print a document, you would choose your network printer and click to print. At the network layer, the printer is always reachable whether you need to print or not, as long as it's turned on and connected to your Wi-Fi. You don't need to enter a password in order to access the printer resource. In other words, there is no authentication and authorization process for access.

The same resource access process is often applied in larger networks within companies using a trust-but-verify model. Once you have logged in with your work-provided secure connection, such as a VPN, you are now free to use the company's resources as if you were sitting in the office. With this model, a single security layer authorizes the user and provides him or her with full access to the entire network as a trusted network user. This allows employees to work remotely uninterrupted.

In the end, too much trust is given to that single component for verification—whether it is the firewall, the VPN, or an internal portal password that protects all of the company's internal documentation. Trust-but-verify is like trying to protect a city from spies using only a wall. Once the spy passes this wall, the key to your kingdom is at risk. The spy can now go stealth, and the detection of abnormal behaviour in your network will likely be more

difficult for your network-monitoring and security teams. Sophisticated attackers access data in non-suspicious ways and exfiltrate data slowly and covertly—often by using new techniques unknown to even current security products.

THE ZERO-TRUST MODEL

In a new approach to security, called "zero trust," your company's network is considered hostile and no resource or asset is considered trusted. With this approach, the general assumption is that the network or a server—internal or external—is likely already compromised or will be the source of a breach at some point. Consider the situation of an unauthorized user trying to access the printer on your network. In a zero-trust network, the printer would not be accessible for printing for anyone—internal or external—without proper authorization.

Zero trust might seem like the obvious approach to heightened security, especially when we hear about attacks on a near daily basis. However, the adoption of this approach has been slow, mainly because implementation requires a major shift in mindset and practice.

A NOTE ON ATTACK INTELLIGENCE

With zero trust, the assumption is that breaches either

have happened or will happen. In most cases, the breach was a result of human intention. In some cases, an automated program, called a "bot," designed to scan and report findings to an operator, is the attack culprit. These two types of breaches have different levels of intelligence.

Automated attacks via bots harness a lower level of intelligence as they typically target loosely configured services. They might scan for IPs, known vulnerabilities, or weak administrator passwords of known services. Some automated attacks are more complex, but they always have limitations due to pre-programmed conditions; they either execute successfully or they halt. For example, a bot might scan for an OpenSSH service, which is usually listening on port 22 TCP. If OpenSSH has a different port than the default, the automated bot might fail, thinking the service is not running on the target host.

Manual targeted attacks, on the other hand, are launched by skilled humans. These are more intelligent than automated attacks as they are specific and sophisticated in their approach, and thus much more dangerous. Changing the port would not prevent or slow down a targeted manual attack.

Companies using zero trust will have a better chance of surviving an intruder on their premises since lateral move-

ment is more difficult—whether the attack was automated or manually deployed.

THE MODEL PROVES ITSELF

At DEFCON, we run hackathons on a regular basis. In a recent hackathon we hosted with Symantec, we quickly saw why zero trust is so essential.

For the purpose of the hackathon, we created an environment that was vulnerable by design. We did this so that the participants could probe and find vulnerabilities, thereby gaining team points. From an architectural perspective, we needed to design a network that was vulnerable. However, it still had to be controlled to some degree, so as to not impact the infrastructure. To achieve this, we made sure that if any one server was compromised, it could not communicate anywhere else, even though all of the servers were part of the same network.

What we were not prepared for was our own mistake. We overlooked a server network configuration, which resulted in a vulnerability that allowed direct access to the server. Sure enough, someone gained direct access early on in the hackathon. However, that person did not have access to the whole environment because the server was not trusted by other servers and could not communicate with the rest of the network.

When we initially planned the systems for the hackathon, we took into account the real possibility of us making a mistake. Even though we weren't purposefully trying to introduce a flaw at the server level, we did. With this critical error on our end, zero trust proved itself. The hacker could access one server, but he could not communicate with the other servers, or even use the credentials he may have found for other users. He couldn't manoeuvre in any way, and the problem was quickly contained. For the purpose of being fair toward the other teams, we did not patch the vulnerability. We may have lost the battle with the individual server, but we did not lose the war.

From the start, we treated the entire environment like one big hostile network. We didn't trust anything coming in or going out, especially since we were dealing with over one hundred hackers simultaneously. Using this zero-trust approach, we knew something could (and probably would) be breached. By using this approach, we minimized the impact caused by a breached resource, which could have been used as an entry point to other areas in our game environment.

A company can easily make the same kind of error in their environment without ever realizing the vulnerability ever existed. Small flaws like these are the reason why companies get breached. The hackathon reflected a real-life scenario.

Through engaging with the security community through DEFCON, I have observed that many people working in the security space in Canada have a high level of awareness when it comes to cybersecurity concerns. However, many companies still have a hard time transitioning fully to a zero-trust model. To transition fully, a company has to invest time, and potentially money, into understanding the internetworking components of their network—their data and their data life cycle.

THE DATA LIFE CYCLE

Zero trust allows a security team to reduce the impact caused by a breached host or network. To use this model effectively, a security team must understand what data they have and their data's life cycle.

If you're a bank, you might want to protect customer data or credit card numbers. If you're a marketing company, your crown jewel might be your list of top customers. Tech companies might want to protect their in-house source code. Coca-Cola would not want to leak their secret recipe. Whatever this most important data is, it needs to be carefully reviewed. What is it? Where is it? How is it moving? Where is it moving from and to?

DATA CLASSIFICATION

Most companies use three major categories to classify their data: public data, private data, and most sensitive data. Based on the data category, you can then know how to maintain, secure, and when necessary, dispose of the data.

If you were to use zero trust, you might wonder why data should be classified at all. Shouldn't all data be protected at the same level? While zero trust will help you develop systems that go beyond one level of verification, every company still needs to be practical. Data cannot be completely removed from the picture. At some point, employees will need some level of access to the data, directly or indirectly.

Classification helps you better identify clearance or access levels that need to be created. Some people in the company will naturally require more privileges than others. Data classification will dictate how the resource hosting the data will be accessed, by whom, when, how, and from where.

When it comes to classification, security and usability sometimes clash, but zero trust doesn't have to be difficult for your users. If implemented correctly, the end result should be both high security and high usability.

DATA WAREHOUSING

With data warehousing, you determine where data should be located and how it should be stored. Security teams should ask questions such as: Which servers or environments host the data? What is the data classification? How is the data being stored and accessed?

One common way to provide permissions and access levels is by using the "least privileges" principle, which at the very basic level dictates that access should only be given up to a point and not beyond. For example, if a salesperson needs to access a shared drive, he or she should only be given access to the sales team's shared drive. Sometimes, the situation is more complex. Even in a shared drive scenario, you may have different datasets, which may require different access levels at the folder level. For example, sales managers may not want their salespeople accessing certain folders, and HR would not want to allow employees access to their colleagues' pay stubs.

When technical difficulties arise, system administrators often resort to the "allow all" access level. This is understandable when someone on the other end of the phone is vehemently complaining that they can't work and are blocked due to insufficient privileges. If you have ever been in a system admin position and had someone complaining about not having enough permissions for

file access just before a client demo, you would understand. In such cases, access is given, but it is rarely taken away efficiently.

The more senior you are in a company, the more privileges you end up with. When employees move from one department to another, they rarely get their old permissions revoked. One solution to this problem is profiling employees based on their permission levels. When they get to a certain permission level, a system flags them and notifies you so that you can revisit their access levels. This methodology can be used in conjunction with a zero-trust model in order to determine whether someone should have access to certain areas in the database or to other resources.

DATA IN MOTION

One reason data can be so difficult to secure and maintain is because it is often in motion and shared. It is being transferred from one place to another. Companies export data, store it in the cloud, or even share access with a separate company, third-party vendor, or contractor. Cryptography is the primary method to move data securely from point A to point B, but what happens after it reaches point B? Your vendor's security practices could have a direct impact on your data. Issues arise with supply chains, which provide a side-channel attack vector, by which someone can access your data without hacking you directly.

To ensure data in motion is protected, you must know how your data flows. Take a publicly facing website, for example. This website will typically communicate with an internal database that is not publicly accessible. By knowing how the traffic traverses your network, you can then ensure that the channels between the server, database, and the customer who accesses your website are encrypted as needed.

In larger companies, a security team may consist of multiple sub-teams, and often there will be a dedicated data security team responsible for knowing where the data is flowing. Banks conduct regular security audits of their web applications and platforms and are usually required to conduct an additional security audit by an independent company in order to ensure they are addressing any potential gaps and possible vulnerabilities. Having an outside organization look at how your data flows can be beneficial. Bringing different skillsets and fresh eyes can yield different results and can greatly improve your security posture.

Consider a simple example of auditing an intranet website that uses a very basic registration process and authentication mechanism of a username and password.

The first thing we want to know is what data we are trying to protect. In this case, it is the credentials themselves.

These will eventually end up in a database, and it's important to understand the full data cycle.

1. Users browse to the website.
2. Users register to the website.
3. System connects to a database and stores the credentials there.
4. Users log in to the website with their new credentials.
5. System goes through a process of validating if the password is correct.

From a data in motion perspective, there are many questions we should be asking:

1. Is the website using a secure channel (HTTPS)?
   A. Is there a component that decrypts the traffic before it reaches the web server, such as a reverse proxy with SSL termination?
   B. Can it be forced to use a non-secure channel (HTTP)?
2. Is the registration process carried over HTTPS?
   A. What encryption protocols are supported by the server?
   B. What HTTP method is used?
   C. Can it be forced to use a non-secure channel (HTTP)?
3. Is the connection between the web server and the database encrypted?

4. Are the same countermeasures of the registration process applied for the login process?
5. Can the connection be downgraded to use weak encryption such as SSLv3 (i.e., POODLE attack)?

There are potentially more questions to ask, depending on the environment, networks, servers, and software stack involved in this scenario. This example shows you that data has to be protected at many layers, and best practices should be applied to ensure data in motion is handled securely.

Let's assume that this website is no longer needed by the company, and we now need to decommission the server completely. What do we do with the hard drives? This leads us to the next phase in the data life cycle: data destruction.

DATA DESTRUCTION

Data shouldn't be accumulated in databases indefinitely. At some point, you might want to or need to destroy unnecessary data in order to reduce the attack surface and to decrease the impact of unauthorized access. Or perhaps you need to safely decommission an antiquated system that once hosted sensitive company information.

Data destruction is divided into two groups: physical

destruction and logical destruction. Physical destruction generally involves a hammer or some other heavy object, explosives, incineration, and high voltage for chipsets. Logical destruction is accomplished by erasing or overwriting data using either software or hardware. Zeros and ones replace the data on all the sectors of the device.

Different media types require different methods of destruction. Sensitive data doesn't necessarily have to be in a digital form. Secrets and sensitive information can be on paper, too. This is where data shredding comes into play.

It is important to familiarize yourself with the different media types: solid-state drives (or SSDs), magnetic tapes, CD/DVD-ROMs. All have different methods of destruction, such as degaussing or breaking CDs into small fragments. SSDs require incineration, and thumb drives require brute force; their internal circuits need to be broken into small fragments. Different media types should all be taken into consideration in your data destruction policy to avoid the possibility of recovery.

Each company should have a robust data destruction policy as part of its data life cycle to ensure data is safely destroyed and permanently unrecoverable. This is important because there are niche vendors who offer specialized data recovery services. Data recovery is an art form in

and of itself, as such vendors can sometimes retrieve data from media previously thought to be destroyed.

Think of a situation where a staff member overwrites and then gets rid of a few disks, but someone manages to retrieve them out of the trash and hires a data recovery expert to salvage the data that was on them. This is where data classification levels are important as each class of data needs to correspond to an appropriate method of data destruction. The destruction of sensitive data needs to be carried out by specialist vendors who can verify the complete inability of recovery and issue a certificate of total destruction.

By understanding your company's data, how it is stored, and where it traverses in and beyond your network, you will be equipped to effectively implement a zero-trust model of security. Greater visibility of your data will not only support your security efforts, but it will help you uphold your reputation as well, a topic which we will explore further in the next chapter.

CHAPTER 8

PROTECTING GLOBAL BRANDS AND REPUTATIONS: AN UPHILL CHALLENGE THAT DOESN'T NEED TO BE

DOLEV FARHI: LEAD SECURITY ENGINEER, PAYTM LABS, FOUNDER, DEFCON 416

Dolev Farhi is an information security engineer who specializes in Linux/UNIX security, web application security, and offensive security. Since starting his security career eight years ago, he has worked for several security firms, including CyberArk and F5 Networks, and provided training for official Linux certification tracks. He is currently employed by Paytm Labs, which builds technologies that power Paytm, the world's fastest-growing mobile payment and commerce ecosystem. Dolev is a founder of DEFCON Toronto, a popular Toronto-based hacker group. He holds several industry-recognized certifications, such as CISSP, RHCE, and LPIC-3. He also manages the largest Linux infrastructure and security community forum in Israel. In his spare time, he builds Capture the Flag challenges for DEFCON Toronto.

Whether we know it or not, cybersecurity professionals are in the business of brand protection. That's really what we do. Think about the tremendous amounts of money organizations spend on marketing, sales, and advertising; what they're spending is creating their brand. What's remarkable is how quickly a brand can be eroded or destroyed via cybercrime. If you lose the confidence of your constituency or your customers, your organization could fail. Reputational damage can be devastating and, unfortunately, a cyber breach can cause irreversible damage. —Ajay K. Sood

Working at a very large bank, I have come to realize that one of our most important objectives is to ensure our reputation is upheld. This objective is achieved in many ways. For example, to show how seriously we take security awareness, we have a security channel publicly available for anyone to report issues. Increasingly, reputation is governed by the way we communicate when something goes wrong.

The reality is that all companies today face security concerns, but most will not publicly discuss those concerns for obvious reasons. When a company gets hacked, customers, vendors, and partners will all want to know the what, when, and how. Is the company prepared? I would argue that readiness is a key part of security, not only from a technical perspective, but also from a communication perspective.

Global brands and large companies often have an old-fashioned approach to communication regarding anything security-related. Today, more so than ever, everything is connected, and updates happen in real time. Companies cannot hide behind corporate building walls when a security or a privacy concern is raised, whether the concern is related to a product they sell or a service they offer. The public is demanding fuller, clearer communication, and companies must respond in a timely manner.

In this chapter, we will consider how to respond to two kinds of scenarios: a typical security incident and responsible disclosure by an external party.

THE INEVITABILITY OF A BREACH

In the previous chapter, we discussed the importance of the zero-trust model. That model assumes the inevitability of a breach.

With typical trust models, "public facing" servers are set up with the highest security practices, oftentimes governed by an advanced network security component. The public website is, after all, accessible and can potentially attract uninvited visitors. One mistake in configuration would result in the attacker being one hop away from the company's crown jewels.

The problem is that other servers in the same network are not given as much attention from a security perspective. Patching is done less frequently, configuration is looser, and more people have keys and passwords to these servers. If you are the unlucky company to be in the crosshairs of a malicious actor, it's just a matter of time. They will eventually find a way through your existing layers, and once in, they will move laterally until they get what they want.

Statistically speaking, there have been exactly 7,339 vulnerabilities reported to the National Vulnerability Database (NVD) from April 1 to July 30, 2018. How many vulnerabilities go unreported? In some cases, vulnerabilities exist but are not reported to the software developer. This is known as a "zero-day vulnerability." Without the vulnerability being reported, how can you protect yourself? Many products on the market build a "normal activity" profile and look for any suspicious behaviour or abnormal patterns and block accordingly. However, normal activity is not a silver bullet and shouldn't be treated as one.

Breaches don't necessarily have to involve customer data. A breach can have a narrow scope. For example, a server might go down without any impact to customer data. Regardless, when a breach does occur, you need to be able to answer questions: What caused the breach? What did you do to fix it? What did you do to make sure

that your customers know about the breach? What did you do to make sure that the leaked data was encrypted? How did you improve your defences?

Many companies tend to remain quiet when they get breached. With the power of social media, and the public's security and privacy awareness, the tendency to under-communicate can backfire and cause viral escalation, leading to a PR nightmare.

AVOIDING REPUTATIONAL DAMAGE

With any breach or security concern in general, the worst response is to be cryptic or to not communicate with stakeholders. To avoid reputational damage, you must be prepared to come up with clear statements about what happened, what you learned, and what you are doing to fix the situation.

A big part of avoiding or reducing the potential reputational damage is being able to communicate simply and honestly. It's important to remember that not all customers are technical, yet they still deserve to know how they were impacted. You want your audience to easily grasp what happened.

Recently, an incident on social media involving T-Mobile Austria surfaced. This was a great example of how, even

without a breach occurring, a company's security practices could be questioned by concerned customers solely due to poor and inaccurate communication sent out from T-Mobile's official Twitter account.

In this case, a T-Mobile Austria customer raised her concerns on Twitter as to how T-Mobile exposes parts of customers' passwords to technical support representatives as part of their identification process. Over the phone, the support representative will ask, "What are the first four characters of your password?" In this way, he or she will be able to verify the person. When the woman tweeted out this information, it went viral. Naturally, and for good reasons, the tweet raised concerns as to how T-Mobile practised security and how they maintained the privacy of their customers' data.

T-Mobile Austria uses its own Twitter account to communicate with its customers. The person managing the account at the time provided a very poor response, saying something like, "Do you even know how telecommunication companies work? We're very secure. We cannot be hacked." This was not only a misinformed response, but it sent the message "Please hack us and prove that we are in fact hackable." Hacking is like a puzzle, a challenge that many people want to solve. For a company to claim publicly that it is resilient to attacks is a digital death wish.

When someone from an official T-Mobile Twitter account

is sending that kind of message, it points to an internal problem. For communication to be effective and technically correct, the security team needs to be involved in order to provide technical information that makes sense. Otherwise, experts will be quick to call out the company.

This lack of professional communication caused a great deal of reputational damage for T-Mobile, even though no breach had occurred. They could have communicated how they protected their customers' data and assured the public that they would begin masking passwords, or that they were looking into alternate ways of user verification. Instead, the unprofessional and misinformed response caused negative Twitter and media attention and generated a substantial problem for the company.

These days, it is imperative that you continuously monitor social media platforms. If it is your marketing team that primarily utilizes social media for your company, establish a strong relationship with them. They should always be prompted to reach out to you about any publicly discussed security concerns, and you should have a regular pulse on any relevant online discussions.

COMPANY RESPONSIBILITY

When a security issue is made known to a company, an incident-handling process should ideally be initiated

to minimize the reputational impact. In many cases, breaches must be reported as part of regulation rules, especially for banks.

Of course, the level and timing of communication does depend on the situation. In general, if the information affects customers in some way—a customer information leak, a password leak, or something similar—you will want to first do a thorough investigation on the scope of the breach. Who is impacted and to what degree? Only after realizing the full picture and scope should an email be sent to those who are impacted.

One ground rule is to not try to sweep it under the rug. Some companies send an "action required" email. In it, they say, "We found suspicious activity in your account, and we advise you to change passwords." This kind of message will likely cause a lot of attention and suspicion. People might wonder if you were hacked and are trying to mitigate the problem without revealing exactly what happened.

Recently, Twitter announced how a misconfiguration of an application resulted in users' passwords being logged in with plain text (unencrypted form). People appreciated that Twitter let them know about the vulnerability. However, when customers started asking questions on social media, Twitter's CTO responded by saying, "We didn't

have to tell you about it, but we did." The back-and-forth here shows that the company has the power to control the level of communication. However, where you set that level depends on you.

A NOTE ON THE DARK WEB

Imagine ten thousand tweets of a direct download link to your customer's database. How long do you think you have to communicate an official message before it hits the news? As you consider how to maintain reputation, think about what you can do upfront to protect yourself. Strive to be the first one to detect any leaked information. It's important to continuously monitor both internal and external resources to do this. Feed monitoring and public dump websites such as Pastebin.com are usually where data is anonymously dumped. Detecting the leaked data early gives you an edge and more flexibility to respond.

The dark web is where a lot of criminal activity happens. The technology it is built on makes it difficult to trace information movement back to its source. It is also a repository for data leaks and illegal offerings, such as stolen credit card numbers with their CVVs.

Finally, the dark web is a source for potential vulnerability feeds that are not easily searchable on the "surface web" or the internet that most of us are familiar with. For banks,

it's a great resource to find fraud campaigns, for example. Vulnerability feeds can help you build better defences.

Police often gather intelligence by conducting undercover operations. They will sometimes embed themselves into criminal groups, pretending to be criminals in order to collect valuable intelligence. They know they can't simply wait for phone calls if they want to keep up with organized-crime groups. To some degree, the same reasoning applies to the cybersecurity space. As a defender, you want to know what the threat actors do in order to better prepare yourself. Creativity is key to staying ahead of the game.

It's a good idea to have someone in your company keep an eye on the dark web for threat intelligence. You might also consider using certain products specifically designed for dark web monitoring. Finally, it might be worth hiring experts in this area to support you and to help you build this monitoring foundation. As with penetration testing, an outside company has a different mindset coming in. They not only have a particular skillset, but can also look at the landscape more objectively.

RESPONSIBLE DISCLOSURE

"Responsible disclosure" is when someone external to the company brings to the company's attention a security or privacy concern. The reporting happens privately,

allowing the company to fix the issue before the problem is published or found by other people who may have malicious intent. Responsible disclosure is typically done by security researchers as part of a "bug bounty" program or a security reporting program.

Responsible disclosure is important because it encourages researchers to disclose issues in a secure and responsible manner, while not putting the company or their customers at risk by publicly exposing their flaws or publishing an exploit.

THE WRONG RESPONSE

There is no consensus on how to handle responsible disclosure. In certain cases, reporters are threatened or even punished by organizations after they've responsibly disclosed security issues. This happened during a voting cycle in the US state of Georgia. An individual found an opening in a website that leaked the information of nearly seven million people. He responsibly disclosed the information to the entity that owned the government website and was reprimanded and punished for his efforts.

Legislators in Georgia then tried to create a bill that would prevent computer snooping, regardless of the intention. They argued that the very finding of a vulnerability should be considered illegal, whatever the person's intent.

While this man clearly did what was right in terms of disclosure and reporting, the case is sometimes not so clear-cut. For example, a nineteen-year-old from Nova Scotia recently found something suspicious on a government website. As he viewed his document, he noticed his ID number at the end of the URL. He changed the number on the URL and was able to view a different document. In this way, he was able to access many different documents that did not belong to him.

In this particular case, the young man did not responsibly disclose. Instead, someone found out what he had done, and he was reprimanded. In his defence, he said he had no malicious intent and did not use the information in any way. Nevertheless, he was reprimanded. There is now a crowdfunding campaign aiming to pay for his legal costs.

Some companies have the wrong response when information is responsibly disclosed to them. They might respond with, "Why did you look into our systems? Now we will sue you." In fact, there is a website that lists security researchers who reported issues responsibly and received threats instead of thanks. As the list grows, researchers grow fearful because they are unsure of how certain companies will react to their report, especially companies that have no previous experience working with researchers.

Recently, I came across a wrong response from a security

company that builds password managers. A researcher found a bug in their vault, and a journalist posted a blog about the bug. The company, in turn, filed a lawsuit against the journalist. Later, someone else found two more flaws in the company's system. Knowing what had happened to the journalist, the researcher tweeted about the flaws. He did not want to report them to the company for fear of being sued.

The company's response was unacceptable, especially especially for a security company. They would have been better served by addressing the vulnerability head on. Instead, their response destroyed their reputation, which ultimately led to lost business as customers automatically disqualified them based on their tarnished reputation.

As security vulnerabilities are here to stay, companies must own their mistakes and clearly communicate their plans for improvement in order to maintain their reputations and remain competitive.

THE CASE FOR RESEARCHERS

As a company, do you want to prevent someone who has good intentions from disclosing information to you? To address responsible disclosure, I advocate utilizing security researchers who intentionally look for bugs on your site or in your system on your behalf.

Leveraging public knowledge to improve your company's defences is a great way to overcome the security talent shortage problem while maintaining minimal spend. The model is proven, as hundreds of security vulnerabilities are reported and patched, resulting in a tremendous return on investment. Companies realize that those with malicious intent will never disclose their findings anyway, as they can use the information in many nefarious ways: phishing campaigns, fraudulent websites, sophisticated attacks that abuse certain software, and more. Having an army of ethical security testers can help sway the odds in the company's favour.

Many large companies like Uber and Facebook have "bug bounty" programs. Such programs pay security researchers who find security flaws. Reward amounts differ depending on the severity of the issue. Anybody can participate; the only requirement is that researchers must responsibly disclose whatever information they find. Some companies have standardized bug bounty programs. Some companies will even run bug bounty programs on your behalf, so that you don't have to manage the intakes. These companies handle reporters, triaging, and payment. They determine eligibility for payment and information disclosure in a secure manner. They have rules around what researchers can and cannot do. With hundreds of people looking for bugs on a website, much can go wrong. These companies also provide ground rules to ensure no

harm is done to your site as a result of scaled running of the program.

It's important to remember that you can leverage the public's curiosity and skillsets to your advantage. If someone finds a bug or a security issue, he or she is compensated. In return, your company's systems are constantly being probed by hundreds, perhaps thousands of people. It can be a win-win for all involved. Companies who utilize researchers can potentially reduce their attack surface, and the return on investment is convincing, especially when your program attracts top talent.

THE CONNECTION TO OPEN SOURCE

Leveraging security researchers' skillsets to probe your systems for defensive purposes can be highly valuable. Think of it as a large QA team on steroids! Similarly, with open source, you invite people to check and use your code. In turn, you can greatly improve the code's resiliency over time. Why is it that we know how modern encryption algorithms work, but they are still difficult to crack? Whereas legacy encryption systems relied on the obscurity of the algorithm, modern systems are open source, making them highly resilient.

Companies such as Microsoft historically embraced closed source, until they realized that the world is head-

ing in the opposite direction. Today, companies are using more open source than ever before. Even Microsoft is adapting. They have come up with their own Linux versions and they also contribute to open source. They even open-sourced their Edge browser's JavaScript engine, Chakra. The world is clearly shifting to a new, more open model across the board.

INTENTIONS

Much of this discussion revolves around basic ethics. If you find a wallet on the street, will you pick it up and put it in your pocket, or will you try to return it? As we look at responsible disclosure, we're asking a similar question. If you notice something that no one else has noticed, what are you going to do with your discovery?

Someone with malicious intent may keep the information and sell it on the dark web for a profit. This kind of malicious intent was seen recently with a case concerning Uber.

An Uber hack was revealed not too long ago, but the actual hack happened back in 2015. Hackers accessed a large portion of customer data and ransomed Uber for $100,000 to remain silent. Uber paid the hackers, but the criminals released the data anyway. Of course, Uber did not handle the situation properly, but they were also dealing with criminals with malicious intent.

Sometimes, a researcher starts on the "good side," but then realizes that the data could be worth substantial amounts of money. Then they consider turning to the "dark side" and use the data to extort money. This scenario is more probable when the person does not receive the level of compensation they feel they deserve.

PROPER REWARD

When researchers are not properly rewarded, you run the risk of the data being disclosed publicly—to competitors or maybe even to the government. When a researcher says, "I'm expecting this amount," that is not necessarily a threat. They don't know what will happen, but they are expecting something. In this case, the company needs to take a political approach. The company might say, "We have a bounty program and offer different amounts of money depending on how critical we find the issue." Researchers need some assurance that they will be rewarded fairly.

A few days ago, I came across a story about someone who found a way to alter Google results. He could get a brand-new website on page one of Google's search engine. Obviously, he could have made an enormous amount of money offering this service to SEO companies. Instead, he did the right thing and disclosed the issue to Google. The report was validated, and Google fixed the issue. As a reward, he received approximately $1,500.

In this case, the man did not feel properly compensated. He could have used his discovery for significant financial gain, or he could have used it for malicious purposes, getting any number of sites to the top of the search engines. Consider how any number of malicious websites could have been bumped up to page one of Google's search engine by running a simple search like "order pizza online." This flaw could have been abused in so many ways.

Because a proper reward was not given, conversations began to question if the concept of responsible disclosure was financially worthwhile. The confusing part to this story is that Google has a bug bounty program. They have paid a lot more money for far less important issues that caused less impact. For an issue this severe, their payment was not sufficient. As a result, researchers may be less inclined to responsibly disclose to Google in the future.

How you communicate with the world can either improve or destroy your reputation. It's important to acknowledge that security and privacy are now in the forefront of the media's attention. If you handle sensitive data, you should become familiar with the industry's ever-changing standards regarding security vulnerabilities and public information communications.

CHAPTER 9

MANAGING MULTIPLE VENDORS AND VENDOR CHURN

MIKE REDEKER: VP AND CIO, CANADIAN PACIFIC RAILWAY

Mike Redeker was appointed vice president, chief information officer (CIO) of CP Rail in October 2012, previously holding the position of CIO at ATB Financial. As CIO, Mike is responsible for redefining CP's future strategic IT roadmap, improving asset utilization, market growth, shipment management, and employee productivity. With over five years at ATB, Mike completed an end-to-end technology upgrade and replacement program. He also spent eleven years at IBM Canada, where he focused on delivering quality information-technology services within the financial services industry. Mike is a graduate of the Northern Alberta Institute of Technology.

Building solid partnerships with vendors you trust is essential in cybersecurity. In fact, how effective you are at building solid relationships with your security providers and vendors is going to dictate how successful you are in the cyber war. Not all vendors are created equal, and each vendor relationship is a unique two-way street with inputs and outputs on both

ends. This chapter explores how to evaluate all your suppliers and assess your relationships with security vendors; it will examine the criteria you should look at when considering which relationships are worth nurturing and keeping, and which ones you should leave behind. —Ajay K. Sood

In order to identify and manage the right security vendors for your organization, you need to have a clear understanding of the life cycle of most products in this space today. You also need to know how to effectively evaluate vendors up front and how to continue evaluating them over time. The goal here is to develop strong partnerships that last.

First, we need to understand that the field of cybersecurity is highly dynamic. New companies emerge in this space on a regular basis. New technologies emerge as well—whether they are built for the purpose of attacking companies or built to respond to those attacks.

In innovation hubs like Silicon Valley, Israel, and Waterloo, Canada, technology vendors are coming out of the woodwork with innovative approaches to combat cybercrime. The problem is that few of these vendors' technologies are integrated into other products. Most of the technologies start as standalone products, but most don't remain that way. Soon enough, a larger vendor will incorporate the new feature into their product as a core requirement.

This product-to-feature life cycle occurred when sandboxing came onto the scene, pioneered by companies like Norman. Their product, Shark, would effectively allow you to execute binaries and study the effect of the execution. Sandboxing allows you to determine, by execution, if code is malicious or not. Before sandboxing, security companies would rely heavily on signatures—the matching of files against a malicious database whenever something new enters the environment—which meant there would usually be at least one successful exploit or infection.

Initially, sandboxing technology was a standalone product. Other companies would put it in-line, alongside their firewall, proxy, and security stack to enhance the security of their aggregate posture. Without sandboxing, criminals could bypass certain security controls, and companies recognized that they needed to add this analysis. The code was smart enough to execute in real time, not simply respond to a database query. As an industry, we were integrating these innovative sandboxing products into our overall security fabric.

Over time, however, firewall, proxy, and gateway vendors began to integrate sandboxing right into their own platforms.

Across the board, startup companies that first innovated and created these standalone products either withered

and died or got acquired by bigger companies. A lot of consolidation occurred in a short period of time. Today, there is an ongoing evolution of emerging technologies, moving from product to feature, and you have to know what is worth your investment. At major tech conferences, like RSAC, there are hundreds of anti-cyber-malware vendors, each with its own approach.

I pay close attention anytime my CISO walks into my office and says, "We need to spend X amount of dollars because what we have today is no longer as effective as the new product on the shelf." At a minimum, we need to explore the associated risks and benefits. A key aspect of my job as CIO is to ensure that the organization is not vulnerable to attacks that could impact our reputation or bottom line. As well, I need to identify which companies have longevity and vision. Will their products be strong enough to remain relevant, whether through an acquisition or merger?

IDENTIFYING THE RIGHT VENDORS

I don't ever believe I have everything 100 percent locked down in our organization. Products change, environments change, our people change. As we move through change and face greater possibility for errors, relationships with the right vendors are of utmost importance.

With larger companies, the vendor relationship often

begins primarily between the vendor and the procurement department. The problem is that the procurement department does not understand all the dynamics around cyber. They end up using the same broad-brush approach with security vendors as they do with any other vendor, running the same types of risk profiles.

This is why security executives must be involved at each step of the relationship. You should be looking for a true partnership rather than a "master-and-slave" relationship. To work with a new vendor and to incorporate their technology, you should be asking a few key questions up front: Does the product integrate with other products, or does it stand alone? Does it deal with common data formats? Are the outputs of the product able to coexist with your existing infrastructure?

Other upfront questions you should ask are related to the executive team and the board. If the company has no track record of success or longevity, you may end up investing a lot of your time and your staff's time on a technology that won't last. Many vendors have disappeared from the advanced malware space. They weren't built to last with the right leadership or financial structure. Simple upfront analysis of time in business and financial statements can reveal a lot early on.

As you evaluate leadership, consider whether your exec-

utive team will be aligned with theirs. Do you know their CTO? Do you have a direct line to their CEO? Can the executives on their team have a relevant security discussion with you? When companies get to a certain size, they sometimes focus on the wrong attributes in their hiring practice—looking for Ivy League grads or MBAs. This approach doesn't work in cyber. You need technology-minded people in places of influence. If the security director of the vendor is using management by spreadsheet, it is not likely to be a successful relationship.

Once I identify a vendor I want to work with, I research to understand their go-to-market model. What do they provide? What products do they use? Can they remain agile and shift as needed? What are their guiding principles when working with customers? I always look to get straight to the smartest people in the vendor organization and have a conversation with them. I want to hear what they can do with a product or how they would address a situation. Once you get to the second or third level of questions and say, "Show me," you can get down to the specifics and weed out the non-candidates very quickly.

In your evaluation, you want to also consider innovation. Does the vendor have defensible intellectual property? Many companies never ask this critical question. If a vendor says they make antivirus, the next questions to them should be, "Do you have defensible, unique ways of

doing that? Do they have patents against your technology?" The company without defensible technology can become a commodity overnight. The second Cisco, Check Point, or Symantec comes out with what that company does, that company will become obsolete.

Executives and technologists regularly butt heads when it comes to bringing products into the enterprise. Technologists often see a new technology that, from a "tech perspective," looks remarkable. The reality, however, is that it would be a risk for the company to bring the technology into its security fabric. Again, due diligence is essential. You should only do business with companies that will last, not just those offering shiny new objects.

The most sophisticated security outfits run in-depth risk profiles on every vendor with whom they might do business. This risk profile will check to see if the vendor adheres to best practices, like ISO. If you are outsourcing to them, you need to check to see if they have their SOC 2 certificate. If so, who certified them? Can they provide documentation for the certification? Too many companies get involved with startups with neat technology that frankly won't last long in this world. This results in operational inefficiency, vendor churn, and a lot of instability in environments.

Practically speaking, a CIO should be in communication

with someone at the senior level of the vendor organization, and your internal team should be aligned with their counterparts on the vendor side who will be implementing a product or providing a service.

GENERALISTS VERSUS EXPERTS

I break the vendor pool into two buckets. One group knocks on our door on a regular basis and says, "You should be hiring us to do X, Y, or Z as it relates to a security practice or security product. We can do that better than anybody else." I am always amazed by how many vendors say, "We're the best." To me, that group represents the generalist pool. They might be helpful for general support, but they are certainly not the experts.

True experts don't knock on doors. Instead, you do the research and seek them out. At CP Rail, we take time to ask, "Who are the organizations that get called upon by top companies when there's a breach or other security disaster? Who are the professionals that go in and determine what happened and how it happened?" Of course, these organizations are few and far between when compared to the generalists.

I am fortunate to work with a CISO who eats, sleeps, and breathes all things security. Whenever there is a breach somewhere in the world, he knows about it. He then

searches through public records to identify which organization went in to fix the problem. After some time, we identify a common trend of top organizations. We think about what makes these organizations unique. We then conduct follow-up research. Why do they have the best tool set in the marketplace? Do they have the best and brightest on their team?

A key to building and maintaining the right vendor relations is trust. Three years ago, we purchased a product that monitored security. It provided reports showing what was inside our internal environment. Upon receiving the product, we searched for a partner who could execute red team exercises (red teams operate as criminals, seeking out ways to access our building, our floor, our network).

We considered three different organizations for this task, but the one we ultimately selected was the organization that created the product. They proved themselves very quickly. We asked them to conduct a six-week penetration test, and their report came back stating that they weren't able to access any of our mission-critical environments. They also helped us see where we may have vulnerabilities. Overall, the relationship added value for us, and it also established trust.

As you move through this process to work with the right vendor, it is important you are clear on your definition of

value. For me, I value partners who can help me identify risks and exposures before anybody else does—before people on my team do, before my internal audit group does, and certainly before any predator in the marketplace does.

TECHNICAL ASPECTS VERSUS GOVERNANCE

As you identify and manage vendor relationships, keep in mind that most vendors are not experts in all aspects of security; most specialize in particular areas. Broadly speaking, they either focus on the technical aspects of IT security or on governance. I have not worked with a vendor that is an expert in both areas.

The technical group specializes in tools, monitoring, and technical skills. Here, I look for the brightest minds with the best tools. When it comes to governance, I look for large system integrator organizations—KPMG, PwC, IBM—that really understand corporate protocol. A vendor working in this area might help you establish your policies around ransomware or determine how to communicate security concerns with executives or the board.

CANADA VERSUS WORLDWIDE

Cybercriminals work globally, and so should you. You need to find and partner with the best of the best to build

your defences efficiently and effectively. At CP Rail, we typically look first for vendors situated in North America, simply because closer proximity translates to easier logistics. That said, we never leave out looking worldwide. My aim is always to find the best and smartest, period.

EVALUATING PARTNERSHIPS

Vendors move in and out of organizations for a number of reasons. First, their technology might become obsolete. In other cases, they face financial instability because they are unable to keep up with the times and stay on top of technological requirements.

In cybersecurity, you are only as good as how you responded to your last breach or your last piece of malware. If your partner is not able to execute, you will churn out that vendor. There's no wiggle room.

Because of how quickly things change in this space, you have to constantly reassess vendors. This reassessment should be more aggressive and more regular with security vendors than it might be with storage, networking, or infrastructure providers.

The top three signs that a company is waning are lack of involvement, lack of innovation, and lack of citation regarding zero days, breaches, or research in general.

First, consider if the company is creating a climate of innovation around cyber. Is it active in determining and defending breaches? When you go to security conferences, do you see this company presenting about pervasive topics in cybersecurity?

Second, a vendor relationship gets stale when a vendor does not keep up with innovation to stay current. A lot of companies talk about thought leadership, but does the company know how to respond to the two biggest questions all security executives want to know about a breach: Who was it? What did they get? The company will not be able to answer these quickly and effectively if they are not innovating.

Finally, you should also be looking into a vendor's investment dollars in research and development. Is this company reacting to breaches, reporting zero-day attacks, and publishing about them? Recently, the FBI advised companies to reboot their routers. In this kind of situation, you want to pay attention to who is publishing information about it. Who published the de facto list?

WHEN RELATIONSHIPS NEED TO END

There are times when a relationship with a vendor needs to end. When you see a broad-based change in leadership or among employees, that indicates the company is declin-

ing. If you notice engineers and other tech employees running, not walking, from the company, you know the company is in crisis.

The tech people are the ones with the conscience. They need to fully believe in what they're doing. If they don't believe the product is great and the work is meaningful, they will leave. It's as simple as that. The demand for cybersecurity talent is so high that skilled engineers can go anywhere they choose.

There are times when a partnership can start well and later spiral downhill. This is often connected to finances. A company might begin with great founders, a great idea, great innovation—but then they go public. When the initial team gets paid out, they go start another company. This is why it is so important to look at the executive board up front. You don't want to partner with people who historically make a bunch of money and then leave. In some cases, however, it's hard to see the reality until it's too late. When you do, it's time to end the relationship.

Just as critical as looking at the board is looking at investors. Investors will make the decision about whether or not to infuse more cash into the company, which can directly impact the value you get from the partnership.

From a personal perspective, I advocate against long-term

vendor relationships to avoid being too reliant on any specific company. Keeping in mind that the life cycle of issues faced in security is abbreviated, short-term arrangements with vendors work best. In rare cases, we might have a long-term relationship for one or two years if we know we will be working with a particular product for that time and it requires a licence agreement or subscription.

Some might say, "You're missing out on what the sales rep would quote as a discount for an extended period of time." I would argue from a more strategic perspective, looking at risk versus reward. I'm okay with walking away from discounts on products or vendor arrangements to stay updated with the best solutions and the best teams.

An argument for short-term arrangements is I know that vendors have to turn over their staff as well. Before working as a CIO at CP Rail, I worked on the vendor side of the business. I'm acquainted with how that community works. Vendors are mandated to grow their business, so with a long-term arrangement you might end up with the A-team for six months and then the B-team for the next six. By focusing on a short-term arrangement with specific deliverables, you get clear value from a vendor.

As a CIO or CISO, you must trust your instincts—one of the most important aspects of which is skepticism—when working with vendors. You can't trust everything you read.

You can't trust everything people tell you, even trusted partners. While building trust with a vendor is essential, you must constantly pay attention to potential blind spots—whether related to quality, service, or even pricing.

I would describe Canada as a trusting nation. Generally, I find that Canadians have a trusting mindset. We tend to believe the best of people. However, that frame of reference would be naive in the cybersecurity world. I get paid, in part, not to trust anything.

As CIO, I have to keep our unique cultural stance in mind. I have to be more skeptical at work than I would be in everyday life. If someone is selling me something, I don't just trust them. If our building is secure, I don't believe it's secure enough. Culturally, we would be prone to let anybody in the door who forgot their badge or code. We want to be respectful, but in the business world—especially in security—we wear a different hat.

ADDRESSING NEW ISSUES

While the most important reason to work with vendors is to stay ahead of potential risks and exposures, you may also need to partner with a vendor after a breach or attack.

I am grateful that we have not yet had to bring in a vendor to mitigate a major breach or attack. Someone who does

should approach that situation in two ways. First, look to your existing business partners for help. Your current partners already have a clear understanding of your environment, so working with them will expedite the process. This is a good starting point to address the challenges and put protective measurements in place.

In concert with that, seek another partner to come in and assess the situation. They should ask, "What's going on? How did we get here?"

Again, skepticism plays a role. Choose to doubt that only one partner can find all the problems. Having a second set of eyes never hurts and increases the likelihood that you will not encounter that problem again.

HOLDING YOUR INTERNAL TEAM ACCOUNTABLE

Any vendor is ultimately limited in what they are able to do. That is why transparency is so important. Real experts are able to articulate whether or not something can be done and why. I always listen for, "No, we can't do that, and here's why." Honest conversations are telling.

That said, I am a big believer in my version of the 80/20 rule. If you expect a vendor to fulfill 100 percent of your requirements, you will always be disappointed. If I can get 80 percent at a reasonable price, I can take that and

manage my way around the other 20 percent. It's important to look at what the vendor is not able to do and factor in the associated cost. You have to factor in X amount of money and Y amount of effort.

At one point, we bought a product from a vendor that was able to do a fair bit of security monitoring and reporting. However, when I started asking what I could see through some form of security dashboard, I quickly recognized gaps in what the product offered. For me, 100 percent would have meant the vendor had an out-of-the-box dashboard solution, where I could log on and see how many computers were patched, the current patching status on all our servers, the internet traffic, and more.

My team explained that the vendor didn't offer that kind of dashboard out of the box. So I prodded further. "Are the team members using this product able to see all that information in some way to do their job effectively?" As long as the team using the product had what they needed, we were 80 percent there. The answer was yes, but I still needed to know how information would pass to me and other key leaders.

Knowing that the team liked the product, I proposed that the individuals using it internally create a solution to pass a certain amount of information to me. They were willing to create this solution, and the gap was filled. This kind

of management between vendor, product, and team is often required by the CIO.

This is where I hold my team accountable. I trust my team to have initial conversations with the vendor and report back to me on their capabilities. If my team returns and says they would like to move forward with the vendor, even though the vendor can only fulfill 70 percent of our requests, I say, "Fine, but I'm holding you accountable to get us the results we need with this partner."

I trust my internal team of experts to seek and find the right fit. Even if I'm unsure of the partnership, I trust their judgment. If they think it's the best solution for our organization and shareholders, I'll hold them accountable to define the needs that must be met and make sure the partner delivers on those needs or that they fill in the gaps.

If you have your most talented, technical geniuses in the dialogue up front, you can avoid issues down the road. I have seen far too many partnerships in which a company realized way too late that the vendor doesn't have the right product or services for their needs, and nothing can be done to fill in the gaps.

Ultimately, I hold managers and directors in the organization accountable for the final decision, but I expect all leaders in our organization to be responsive to team

feedback. After all, their teams will be the ones using the products.

CHAPTER 10

DATA OVERLOAD—MANAGING BIG DATA EFFECTIVELY

MIKE REDEKER: VIP, CIO, CANADIAN PACIFIC RAILWAY

Mike Redeker was appointed vice president, chief information officer (CIO) of CP Rail in October 2012, previously holding the position of CIO at ATB Financial. As CIO, Mike is responsible for redefining CP's future strategic IT roadmap, improving asset utilization, market growth, shipment management, and employee productivity. With over five years at ATB, Mike completed an end-to-end technology upgrade and replacement program. He also spent eleven years at IBM Canada, where he focused on delivering quality information-technology services within the financial services industry. Mike is a graduate of the Northern Alberta Institute of Technology.

Organizations have more data than they've ever had before. The challenge is to go through all that data and perform triage and arbitrage to determine whether or not a significant event has occurred. This is a ubiquitous problem that applies pretty much to any and all organizations. They have to review all of the event information and prioritize it.

This isn't even a needle in a haystack problem; it's a needle in a haystack on a five-thousand-acre farm with one hundred haystacks per acre. Which haystack are we going to start with? It's beyond complex. The math is against us when it comes to cyber. You're going to be looking for a single entry of relevance in an enormous field of potentially irrelevant data. —Ajay K. Sood

In the security space, we deal with massive amounts of data daily. As CIOs, we effectively manage big data by turning it into actionable information.

Security organizations have rushed to security information event management (SIEM) systems to aggregate and manage security information. Several drivers led to the need for these aggregation systems. A principal driver was regulatory compliance; organizations were mandated to retain all of their log information for periods of anything between two and ten years, or sometimes indefinitely.

The SIEM would bring together large quantities of event data from disparate places around the network into one central location, providing a single location for all log data. Firewall logs, DNS logs, endpoint logs, access logs, and other data would all be fed into the SIEM. In our case at CP Rail, instead of having numerous smaller data piles spread throughout our 1,600 Windows servers and 1,000 Linux servers, we now have one centralized repository.

Ultimately, since SIEM systems were already storing all of the log information, administrators began to rely upon them as resources to search for security incidents. Originally, this was the extent of their usefulness, but eventually, someone had the idea that they could use these same systems as a way to provide forensic data if an organization was breached. These systems would ultimately begin to integrate machine learning and predictive analytics engines as well, to proactively seek out indicators of compromise.

LARGE PILES OF DATA

If you think of this new pile of information as a large haystack, you inevitably need to look for the needle within it when a problem arises or a breach occurs. The problem is that the needle moves, and the needle is only relevant for a certain period of time. It's not overly useful to know you were breached three months ago. You need to know a breach is occurring when it happens. Ideally, you could have an idea of which breaches might occur before they actually happen.

With a lot of data but no way of knowing what is relevant, you can't prioritize. The reality is that you will always have someone knocking on your door. What you need to know is whether someone has gotten through the door. If a criminal comes to the door, looks in, and then decides

to turn away, do you care? Should you treat that event in the same manner as you would if the criminal got in, went upstairs, and stole all your socks from your sock drawer? That's the real event. If you are highly prepared, the criminal might make it to your sock drawer but then get thwarted by a countermeasure, finally to be caught and arrested.

Whatever the case might be, you need to know if an attack occurred but failed, or succeeded, and to what extent. All of these instances require different levels of escalation, and SIEMs cannot help you differentiate between them natively. This is the big-data problem: the inability to know what data from the pool is relevant and when it is relevant.

REQUIRED EVOLUTION

There has been an evolution in how we respond in cybersecurity. We started with a tools-based response. Then we moved to a human-based response. People would try to respond to every incident coming into their SIEM, and we quickly realized the limitations of human scalability. A company might get five thousand alerts a day, but a human can only respond to twenty to fifty effectively. Of course, you can start writing some rules for common problems, but you can only write so many rules manually; though effective, human-based responses cannot scale. So what comes next?

Welcome to the modern era, in which machine learning (ML) and artificial intelligence (AI) will be able to understand your network traffic—what is normal and not normal—and start to do correlation and prediction, which is now being done manually or via observation.

Right now, if someone logs in from Calgary to a single system and then logs in from Bangladesh thirty minutes later, a human can apply intelligence and decision-making to spot an anomaly. If you are monitoring 50,000 user IDs across 1,000 servers in 200 sites, the problem of interpreting big log data at scale quickly becomes apparent.

In the modern era, two words are especially important: triage and arbitrage. Triage is about being able to sort through all of the data. Arbitrage allows you to make a decision based on what is important to you. You need to be able to respond differently to someone breaking in and stealing your Rolex than you would to someone stealing your socks. While ML and AI can be used interchangeably, ML is most connected to triage and AI is most connected to arbitrage.

SIEMs without some form of decision-making logic could never differentiate between the theft of a critical and non-critical asset. Additionally, they cannot recognize persistence. A SIEM might indicate that an innocuous van is parked in the garage of your house, but it's only

after the house has been ransacked of its contents and the van leaves that it is identified as a potential threat. This notion of persistence, where an attacker has taken root and is waiting for the opportune moment to strike, is one of the more difficult threats to detect and mitigate.

Bringing it back to CP Rail, we collect a total of twelve to eighteen billion events every month. Obviously, it would be impossible to work directly with raw data, so logic must be applied to it. Ultimately, you want to filter for the information from which you can make informed security decisions. To apply the right logic, you can find the right tool and add necessary functionalities to it, or you can build your own tools in-house.

CONSIDER YOUR RESPONSE

Most organizations have an overload of alerts. Some of our most important alerts, for example, come from Active Directory, which provides particular privileges to different groups. We monitor these groups and also get alerts when a user gets added to one of them. Because certain groups have high-level privileges, we always double-check to make sure it's an authorized addition. Every day, events from Active Directory come into our monitoring system, which filters down the events and triggers alerts.

Active Directory is only one of our systems. Alerts come

from all of our networked devices, servers, and applications. A lot of the events are benign, but the sheer amount can seem overwhelming.

It's normal to feel frustrated because of the impossibility of responding to all alerts. What is interesting though, is that the sheer volume of alerts could simply be a distraction. If your team is overwhelmed, they might miss the actual event.

Cybercriminals often leverage the overwhelming nature of alerts as part of their playbook. They will launch low-tech denial-of-service attacks at the external interface of your firewall to cause your team to respond, to look at all the outside-in logs. All of a sudden, there is one encrypted html connection from the inside out. Your data leaks, and nobody knows. Everyone is too busy responding to the distraction.

In this case, the aggregate value of the one inside-out connection is more valuable than ten billion outside-in connections that are failing. Of course, each one represents a line in the SIEM, so each represents something someone needs to respond to.

These kinds of attacks by criminals can feel paralyzing, especially if an attacker has scaled persistence on multiple machines. When your IT department can only respond

to twenty events a day and the criminal has thousands of machines CryptoLocked, you will be busy for months. All the while, the criminals are using this as a distraction from their effort to extract information from your network.

In this kind of situation, it is almost impossible to pull the needle out of the haystack. In fact, the team might be looking for a needle when they should be looking for a wrench. Other times, they're looking for one needle when they should be looking for sixty. You don't know how many problems there are or how big they are until you find them.

PEOPLE, ANALYTICS, AI, AND ML

So how do you get consistently useful and actionable information in today's cybersecurity world? People, analytics, and AI all play a role.

STAFFING AND PARTNERSHIPS

Once you have accepted the fact that the adversary is formidable and could get in anytime, you have to take an honest look at the overall situation and your team's capabilities. Part of the equation for handling data is staffing. When it comes to working with big data, my first approach is to insource as much as possible, due to the specific nature of our business.

Those who are in-house will be familiar with typical alerts and typical events that take place within the organization. For example, our trains cover eleven thousand miles, and we have sensors all along the way. We have bungalows along our tracks, and each one has a device to track traffic. Someone in-house understands what kinds of events these sensors might capture and where the alerts are coming from. That person would immediately notice any unusual alerts and raise an alarm, "We're seeing a high volume of traffic in a given location, and the data doesn't make sense." Sure enough, someone hacked into a remote piece of equipment. When employees understand the business, they understand the information coming through and are able to connect the dots much more effectively.

Every organization will go about staffing and distributing responsibilities differently. At CP Rail, we identify one person who looks at the data coming through in real time and a second person to verify and validate. These roles are critical to the accuracy and usefulness of information we gather from big data.

One of the biggest challenges for our CISO is finding people with the right skills on a regular basis. He consistently runs on a 20 to 25 percent vacancy rate on his team, and yet the team that is present is clearly invested. Still, even if his team is full of black belts, he will need to find the right partners in certain situations, depending

on the level of kung fu the team can respond to on its own. Every CIO and CISO should know when to bring in outside forces.

ANALYTICS AND AI

With analytics, you can take the data you have and run models against it to have a baseline understanding of what is going on, what events have occurred, or where events are coming from. Analytics is all about looking at outcomes that have already occurred.

While AI is principally trying to predict outcomes before they happen, analytics will give AI what it needs to make proper decisions. In the end, arbitrage will be driven by AI in real time outside the analytics engine, but one hand still washes the other.

Over time, we developed a central dashboard that enables our teams—whether operations, finance, or otherwise—to make better decisions. Using analytics, we expose the information at the highest level, and each team can drill down to the lowest level, even to the raw data. For example, our dashboard can show one team the speed of different trains, another team the number of bad order cars on a train, and another team the challenges we are experiencing across North American locations. In some cases, teams can begin to do predictive analysis based on the information they see.

We use the same process within the security department. My CISO and I can look at the dashboard and determine where our greatest vulnerabilities are. We can see where alerts are coming from and begin to evaluate why.

AI/ML

While analytics is limited and based on previous events, AI learns in real time how to treat unexpected circumstances and predict an outcome.

Now that AI/ML is available, it can be utilized to constantly monitor your SIEM and other systems and help you determine when to get a human involved. Without AI/ML, responses from people could go terribly wrong. For example, a Level 1 analyst might know that a machine is running slowly and be able to recognize a CryptoLocker. However, their response might be to reboot or, worse, reimage the affected machine. Meanwhile, no one sees that this was a memory-based attack and all your information was just stolen.

A lot of organizations are not yet confident with AI. The challenge is that ultimately, attackers can and will use AI to breach you. Incorporating AI to help you manage big data or employing the right partner to do it will be table stakes. Machine learning has very specific algorithms. If someone asks what kind of machine learning you are

using, you should have an answer. If you don't, you need to know who does.

AI will be the cyber-munition of the future, much like 56-bit DES encryption was controlled and treated as a munition by certain governments and others back in the nineties. Of course, today we routinely use 256-, 512-, and 1,024-bit cipher strengths for encryption. It's understandable why AI can be treated this way. AI in the wrong hands can be a scary thing. Still, the reality is that criminals will use it.

AI gets magical when it predicts something seemingly unrelated but completely accurate. We see this today with advertising. Google, Amazon, and other major players use AI to predict what you want to buy. They serve up content to you that is relevant. They use more than analytics. They have the ability to predict what you might want next.

Well, let's apply the magic of AI to attacks. What if someone could track your organizational movements of the day? Not only does the attacker know when you get out of bed and leave for work, but the attacker can predict something you will do today that is unrelated to your typical routine, keeping you out a little longer than normal. Before you've left, they're ready to take the house.

That's next level, and that is why AI is so relevant to cyber-

security. Attackers can use it to figure out what techniques and personnel administrators are using to monitor systems, and what countermeasures are in place. They can use it to know if and how a certain office is staffed. If the office is in India, perhaps the attacker will wait until a cricket final and orchestrate an attack while everyone is distracted. The possibilities are endless.

As an organization, we are in the beginning stages of exploring AI. Many organizations are in this same position. Some already have utilized AI effectively, but many are testing the effectiveness of process automation. We currently use AI in our data centre. We foresee AI taking on a larger role and supporting us further with alerts. Ultimately, we hope to use AI to identify historical patterns in alerts and tell us where we should be paying closer attention.

CHAPTER 11

WHICH SECURITY CONSIDERATIONS TO PUT FORTH, AND HOW

AMIR BELKHELLADI: PARTNER, RISK ADVISORY LEADER FOR EASTERN CANADA, DELOITTE

Amir leads Deloitte Canada Eastern Region's Risk Advisory practice and has nearly twenty years of experience in cybersecurity, focusing on strategic advice and leadership of significant global cybersecurity transformation programs. Amir previously worked in France, where he led Accenture's security practice, and in the UK as the chief security architect and group operations chief technology officer for Lloyds Bank, the country's largest retail financial institution.

Every organization, no matter how large, has limited resources. You only have so many executive cycles; you only have so much attention; you only have so much time; you only have so much money. With scarce resources, how do you prioritize how you use them? If it's executive mind-share, what do you communicate to them? When do you communicate to them? There's a lot of info that can be communicated to and from various levels within organizations, but figuring out what needs to be

communicated and when it needs to be communicated can be a challenge. —Ajay K. Sood

A few years ago, an agent with the United States Federal Bureau of Investigation made a comment about cyber-attacks: "There are those organizations that have been attacked, and there are those that don't yet know they have been attacked." There is a lot of truth to that statement. The threats are constant. Cyber-enabled risk is a dynamic environment. Criminals are attacking all the time, and companies are defending all the time. Defence is required twenty-four hours a day, 365 days a year.

As has been discussed elsewhere in this book, a good defence must begin with identifying exactly what it is that you are protecting; putting the people, processes, and technology in place to protect those assets; and being able to respond to an attack if and when it happens. The questions I discuss in this chapter are which security considerations you should focus your efforts on, and how you should organize them. I will outline a security framework including five steps and three elements that any organization can begin implementing right away.

FIVE STEPS OF CYBERSECURITY

The five steps of cybersecurity are identify, protect, detect, respond, and recover. The analogy that I like to use to

explain these steps is a break-in and burglary in a private home. If you have valuables in your home, before any break-in happens, it is wise to identify and document not only all of the valuables in the house, but also where they are. That's step one, identify.

Step two, protect, might involve putting better locks on doors and bars on the windows. Step three, detect, would include some type of alarm system that notifies the homeowner and the police when unauthorized access has occurred. Step four, respond, could mean calling the police and attempting to secure the house once a break-in is detected. And finally, step five, recover, includes everything the homeowner must do to repair the damage, recover stolen items, and get back to life as usual.

Now let's look at these same five steps in the cybersecurity environment. The first step is to "identify" what the valuables are—understand what data and information in the organization is important to guard. This involves first knowing everything the organization owns, then determining what the impact would be if it were lost, stolen, or compromised. Assets should be ranked by importance, with the most crucial assets at the top of the list. These are the crown jewels, to be protected above all else.

Regulations like the General Data Protection Regulation (GDPR) in Europe are important to the "identify" step

because they help organizations understand what information they should be protecting. If a regulatory agency says a certain type of data must be protected, you have no choice but to protect it, even if you do not consider that data part of the organization's crown jewels. Make sure something is protected if there's a business reason or because there is a law or regulation that requires it. Maintaining compliance falls under the "identify" step.

The second step is to "protect" those valuables. This means putting in place all measures and controls to minimize the risk of a data breach. A breach refers to any time an unauthorized entity accesses company data without permission. Breaches come in all shapes and sizes, from both inside and outside an organization. A breach may entail theft of data, destruction of data, encryption of data, or the disabling of systems to prevent the organization from operating. The point of this step is to prevent someone without permission from gaining access to private data and systems.

The third step is to "detect" when there is a breach. Detect refers to the alarm system that alerts an organization to an unauthorized intrusion. This step is usually accomplished through people, processes, and systems working together to detect both attempted and successful intrusions. Despite your best efforts and all the latest and greatest measures and controls to prevent a breach, you still may get hacked.

The fourth step is to "respond." Once there has been an attack, how does the organization react? The key to this step is to be prepared and have a well-organized response plan on standby with established processes in place. It also requires having the right tools to contain the threat.

The fifth and final step is to "recover." This includes everything an organization does after an attack to restore order and to get back to business as usual. This step requires having a good recovery plan with set processes, then testing and practising those plans and processes before an attack occurs so that when a breach happens, the company can bounce back quickly. These final two steps, "respond" and "recover," are what we call breach management.

PEOPLE, PROCESS, AND TECHNOLOGY

For each of the five steps described above, three elements should be applied to achieve the goals of that step: people, process, and technology.

PEOPLE

"People" refers to the humans in your organization, their roles and functions, expertise, and effectiveness. It also refers to the organization's structure and any planning that is done related to cybersecurity. People also includes experts and human resources that reside outside the com-

pany, such as cybersecurity consultants, investigators, and so on.

Some questions to consider when assessing the people element include the following: How many people do we have on the team? Is that enough? How is the team structured? Are our people focused on the right things? Do we have the right people in the right positions? Are we able to recruit and hire the additional people we need?

PROCESS

"Process" includes any set of activities that must be taken, or any series of decisions that need to be made in order to support the overall objective. That goal could be protection, detection, response, or recovery. Think of process like a flow chart. If event A happens, then you do action B. If B doesn't solve the issue, you choose between C and D.

Process can be mapped out like a decision tree. Having set processes makes it easier to handle cybersecurity issues properly and to comply with industry standards. All processes must be well documented, understood by the team, and practised regularly.

There are organizations that can help companies implement process frameworks to maintain compliance and protect data. One is the National Institute of Standards

and Technology (NIST). Another is ISO 27001, which is an international standard for information security management. These are two of the best resources for establishing quality process controls in an organization.

TECHNOLOGY

"Technology" refers to all the tools that help an organization achieve cybersecurity. These might include inventory technologies, databases to track assets, antivirus software, firewalls, endpoint parameter, encryption, diagnostic and automation tools, endpoint detection and remediation (EDRs), and so on.

For example, one of the most potent tools is security information and event management (SIEM), which monitors large volumes of data to detect potential breaches and attacks. GRC tools are technologies that track governance, risk, and compliance. And Symantec has developed host-based intrusion detection system, or HIDS, tools to install on laptops that are like mini alarm systems.

Technology can greatly enhance the power of people and processes to reduce cyber risk. Technology has the added advantage that it doesn't make mistakes—only people do that. The fact is, though, people are the key to cybersecurity. If an organization goes out and spends a lot of money buying the best security tools available, they often

make the mistake of thinking technology is a silver bullet and now they are safe from attack: "We just spent all this money on software and technology; no one can breach us now." That is absolutely not the case.

Great tools without great people to operate them simply will not provide effective protection. People are the most important part of the cybersecurity equation because they operate the tools and follow the processes.

HOW TO BEGIN

So far in this chapter, we've discussed the five steps and the three elements that every cybersecurity plan should consider. But if you are new to cybersecurity, or if you're at a new organization such as a startup, you may have to start at the very beginning to secure the company. Here's how.

Create a document and list each of the five steps (identify, protect, detect, respond, and recover) as a separate header in the document. Under each of the five steps, list the three elements (people, process, and technology) as subheads. To be clear: you will list people, process, and technology a total of five times each, once under each of the five steps.

Begin filling in the document, paying attention to the information we have described in this chapter. The document

you create will serve as the basis of your cybersecurity plan. If you are just beginning this process, you are at level one. You have a long way to go before you are fully prepared for cyber threats.

Level two is implementing your plan within your organization. Put the people, processes, and technology in place and get them ready to function. Level three is where you actually start to run the system and make sure that it's working.

Level four is where you test the system for vulnerabilities and gaps. You shake the proverbial tree. Finally, level five is ongoing maintenance, testing, streamlining, improving, and making adjustments as needed.

MATURITY LEVELS AND TESTING

For all three of the elements above—people, process, and technology—the CISO must assess something we call the maturity level. If a new process or a new cybersecurity manager (CSM) or a new software program has only recently started functioning, we'd like to say that element has a low maturity level. The longer a CSM has been on the job, the greater maturity he or she has, and the better security provided. The same goes for process and technology. The greater the maturity level, the more effective the elements will be. Maturity levels improve over time.

Advanced organizations perform comprehensive testing of people, processes, and technology against all five steps—identify, protect, detect, respond, and recover. They perform intrusion testing, detection testing, specific attack scenarios, and run simulations.

For example, let's say that you have identified your customer database as the key asset you want to protect. You've put in place a team and a suite of technology to protect it, and you have the right processes in place. You then add your detection systems around that, and now you believe you're ready to respond to an attack.

The next step is actually testing the system to see how well it works. You make sure any attempted breaches are detected, contained, and responded to quickly and effectively. We call this exercise "red teaming," and it's a great way to assess your readiness for an actual attack.

SECURITY IS AN ONGOING REQUIREMENT

Many organizations falsely believe that when they've put in place cybersecurity measures and tested them once, they're done. That is definitely not the case. Cyber threats are constantly changing, so testing must be performed regularly.

Once you have put in place the five steps for cybersecurity

(identify, protect, detect, respond, and recover), utilized the three elements (people, process, and technology), and successfully tested the system, you should be well prepared to manage security incidents. Of course, doing all this doesn't mean that your organization is immune to or fully protected from attacks. But it does mean that if a cyberattack were to happen, you have built enough capability within your organization to deal with it effectively.

CHAPTER 12

GENERAL DATA PROTECTION REGULATION (GDPR)

EDWARD KILEDJIAN: VP OF INFORMATION SECURITY, COMPLIANCE AND CISO, OPENTEXT

Edward Kiledjian is the VP of Information Security, Compliance and CISO at OpenText, a global enterprise information services firm with 140 offices around the world. Ed has spent the last twenty-five years in cybersecurity or, as he says, since "long before the industry was cool." He has helped secure organizations in more than forty countries and in a wide range of industries, including transportation, utilities, manufacturing, and government. For more of his insights and opinions on security, check out his blog at Kiledjian.com.

The GDPR is a watershed event in our industry with far-reaching effects that we may not know for years to come. We are still studying its impact, but there has already been some fallout in the form of billions of dollars of lawsuits. The GDPR is an important case study because it's the precursor to potential future legislation in Canada. The framework has already been laid out with Canada's Digital Privacy Act (DPA). We

all need to pay attention to what the GDPR is, what it means for organizations right now, what its impact has been already, and what it will be in the future. —Ajay K. Sood

Crude oil has been one of the world's most valuable commodities since the 1970s. But today it's being supplanted by an even more valuable commodity: data.

Just as oil is pumped out of wells and processed into valuable products that are subsequently sold to end users, something similar is happening with data. Companies mine data from a myriad of sources, process the data to create consumer profiles, and inventory the profiles, ultimately selling them to other companies and end users. A key question that has remained unanswered is: "Who owns that data?"

As with any precious commodity traded across international borders, governments have attempted to impose regulations on the use and storage of data. Until now, those regulations have largely been guidelines, with no teeth or negative repercussions for organizations that disregard the rules.

A tectonic shift has arrived at global data storage and privacy practices. It's called the General Data Protection Regulation (GDPR). The European Union enacted the GDPR in April 2016 and, after a two-year grace period, the

law formally went into effect for all organizations operating in the EU on May 25, 2018. The GDPR is a massive, pan-European regulation of personal data that organizations of all sizes must comply with.

Even though this new set of regulations ostensibly regulates companies in the European Union, you'll see in this chapter why it also applies to all companies and organizations that do business in Europe or with citizens of the EU. In practice, the GDPR is extraterritorial; by design, it can regulate the activities of companies and organizations outside of the EU, meaning all over the world.

The reality of the GDPR is that it empowers individuals, referred to as data subjects, to have more control over their personal information. The goal of the GDPR is to force companies to be clear about their intentions when it comes to collecting personal information. And it forces companies to think about how they're capturing data, how long they're storing data, and what they're doing with the data, and to be reasonable with the data.

IMPORTANT GDPR DEFINITION: PERSONAL DATA

From GDPR Article 4: "For the purposes of this Regulation: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

BACKGROUND

Almost every country has some form of privacy laws governing how companies can store and use its citizens' personal data. For example, the Data Protection Act (DPA) is a British legislation passed by the UK Parliament in 1998. The DPA created a set of data protection principles to make sure personal information is used fairly, lawfully, safely, and only for limited, specific purposes. Similar laws are in place in the United States, Canada, and throughout Europe. Canada's law is called the Personal Information Protection and Electronic Documents Act (PIPEDA).

The problem is that laws passed twenty years ago can't effectively regulate today's data usage. When the British Parliament passed the DPA, deep data mining and profiling were non-existent. In addition, both the DPA

and PIPEDA are basically toothless as neither have real threat of penalties or fines attached. Over the past two decades, both privacy landscape and data technology have evolved, and DPA and PIPEDA do not address the issue of data ownership.

Today, in North America, there is an ongoing debate over who owns personal data. If a private citizen uploads their whole life to their social media accounts, do they own that information or does the social media company own it? This question resulted in Facebook CEO Mark Zuckerberg's testimony before the United States Congress in April 2018. He talked about how Facebook *handles* users' private information. But who *owns* that data is still in question in the United States.

Now that the GDPR is in effect, that question is settled in the EU. The GDPR makes it clear that in every EU country, each citizen's personal data is ultimately owned by that private citizen—not by the company that collected and stored the data.

GDPR QUICK FACTS

If you collect or store personal data about European customers, employees, or suppliers, the GDPR applies to you, regardless of geolocation.

The General Data Protection Regulation went into effect on May 25, 2018.

The GDPR will drastically change how organizations store and use the personal data of Europeans.

This new law has massive repercussions for organizations around the world. Any EU citizen can revoke an organization's right to store his/her personal data at any time. The private citizen can request their data be destroyed, and the organization must comply. Many of the laws before the GDPR were privacy laws, but they didn't shift the paradigm of data ownership. This one does.

Not only does the GDPR turn the data ownership paradigm on its head, but it also has teeth—sharp teeth. Violation of the law can lead to huge fines, potentially into the tens of millions of euros, to ensure organizations do not breach its requirements.

The GDPR is an ambitious and tough set of regulations. Nothing like it has ever been put in place for data privacy. Now businesses, governments, and organizations all over the world are watching closely to see how it plays out.

Let's take a deeper dive into the GDPR to learn more about it and how it will drastically change the way organizations handle personal data.

IMPORTANT: LEGAL DISCLAIMER TO THE READER

It is important to understand that this chapter is by no means an exhaustive review or analysis of the GDPR. It is a summary only. Seek professional, qualified guidance about GDPR interpretation and compliance from a competent attorney. Information provided in these pages is for educational purposes only and should not be relied on.

THE GDPR REPLACES THE OLD REGULATIONS IN THE EU

In Europe, the GDPR replaces the older Data Protection Directive (95/46/EC) of 1995. The GDPR has been set up as a regulation and not as a directive. This means it will be immediately enforceable without individual transposition by member states. It also means all European states will use the same privacy rules and regulations.

EXTRATERRITORIAL REACH

Although the GDPR is a European regulation, it applies to any business working with European data, regardless of geolocation. This is a major change compared to the

current Data Protection Directive that is being replaced. GDPR Article 3 covers this topic and states:

> This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not.

In other words, the GDPR applies not only to firms located in the EU, but also to firms located outside of the EU but that offer goods or services to EU residents, or that collect or process EU residents' data.

There is no size limit on organizations that must comply with this rule. Article 3 applies to everyone from the largest multinational corporation to the smallest Etsy craft-maker shipping hand-carved wood sculptures to the EU. Firms outside of the EU do have the option of complying with the GDPR just for European subjects and using other regulations for non-Europeans. However, running multiple privacy programs can become costly. Therefore, it is expected most firms will use the GDPR globally to simplify their processes and reduce compliance costs.

European authorities created Recital 23 to help clarify whether a firm is considered to be offering goods and services to EU citizens. (GDPR refers to private citizens

as "data subjects.") Some of the factors that may indicate GDPR application include:

- The mere accessibility of the controller's, processor's, or an intermediary's website in the European Union.
- Email addresses or other contact details in the EU.
- The use of a language or a currency generally used in one or more member states, with the possibility of ordering goods and services in that language or currency.
- The mentioning of customers or users who are in the EU, which may make it apparent that the controller envisages offering goods or services to citizens in the EU.
- The firm produces a product in a language that is a predominant language in one of the EU states.
- The firm lists euro pricing for its products or services.

The recital provides a way out of GDPR compliance for firms that clearly do not market their goods or services to EU residents. If you are allowed not to comply based on the recital, you are not expected to implement complicated and expensive mitigating controls like geolocation IP blocking, rejecting mail from EU mail servers, etc.

The recital also clarifies that the use of a major global language—like English or Spanish—in marketing material does not automatically constitute marketing to EU states.

However, if a language is used in marketing that is primarily used within an EU member state (e.g., Estonian), then it is automatically assumed you are marketing to EU residents.

REGULATIONS WITH TEETH

The European Union understands that financial penalties are powerful motivators for companies. Thus, severe fines and liabilities have been designed into the regulations.

Article 83 is entitled "General conditions for imposing administrative fines." It describes the liabilities, fines, and remedies companies may be subject to if they violate the rules. Article 83.5 lists the highest penalty level as, "20,000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher." So penalties could easily reach into the many tens of millions of euros. However, there are some violations which entail the smaller fine of "10,000,000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher."

So how are fines determined? Fines are administered by individual member-state supervisory authorities. GDPR Article 83.1 states, "Each supervisory authority shall ensure that the imposition of administrative fines

pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive." Fines are evaluated using ten criteria:

1. Nature of the infringement—The number of people affected, the damage they suffered, the duration of the infringement, and whether the purpose of data processing was respected.
2. Intention—Was the infringement intentional or neglectful?
3. Mitigation—What actions did the company take to mitigate the damage?
4. Preventative measures—What types of technical and organizational preventative controls did the firm implement? Were they adequate and appropriate for the nature of the data and the foreseeable impact of a leak?
5. History—Is the issue recurring or a one-off issue? Article 83.2 (e) cites "Any relevant previous infringements by the controller or processor."
6. Cooperation level—How cooperative was the firm with the supervisory authority to remediate the infringement and provide support for data collection, and how quickly did the firm comply with response requirements determined by the supervisory authority?
7. Data Type—GDPR Article 9 includes a description of "Processing of special categories of personal data."

All data about Europeans is protected by the GDPR, but there is a special class of data that requires much more protection and can generate much stiffer penalties. Article 9.1 includes "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."

8. Notification—The supervisory authority wants to ensure that notification is done quickly, accurately, and completely pursuant to a breach or leak. Article 33 is entitled "Notification of a personal data breach to the supervisory authority." The crux of the requirement is that the firm must notify the supervisory authority no later than seventy-two hours after becoming aware of a breach.
9. Certification—There are no GDPR certifications as yet, but the supervisory authority will determine if the firm had any relevant data privacy certifications (e.g., ISO 27001 or Cyber Essentials) and will determine if the firm was compliant with the conditions of that certification.
10. Other—The supervisory authority will determine if there are other aggravating or mitigating factors that must be considered when determining the penalties.

If the supervising authority of the GDPR determines that

you are a repeat offender and that you've had an excessive number of breaches, they can impose a temporary processing ban on the data of Europeans. In the most extreme cases, the supervising authority has the ability to impose a permanent processing ban on European data. This means that repeat violations and breaches can escalate from simple fines to the material destruction of your ability to conduct business in Europe.

As such, the GDPR is a powerful law that you do not want to misinterpret or ignore. So I reiterate here the disclaimer stated earlier in this chapter. Everyone reading this section should get professional, qualified guidance about GDPR interpretation from a competent attorney. Information provided in these pages is for educational purposes only and should not be relied upon.

GDPR EXCLUSIONS

GDPR Article 2 is entitled "Material scope" and lists in section 2 instances where the regulation does not apply. As an example, Article 2.2 (c) states the regulations do not apply to data collected "By a natural person in the course of a purely personal or household activity."

It's important to understand that previously collected data is not grandfathered under older regulations. Controllers must obtain consent from the individuals for current use,

or they must cease processing of that data, no matter how long ago the data was collected. There is no grandfathering of data, period.

GDPR DEFINITIONS

GDPR is a very technical law. To fully understand the text and spirit of the law requires a common understanding of a few key definitions. These definitions are provided in Article 4. Important definitions include:

1. "Personal data" means any information relating to an identified or identifiable natural person (referred to as a "data subject"). Personal data includes any two pieces of information that could be used to track down a person. This includes information such as: name, phone number, credit cards, bank accounts, payment information, usernames and passwords, email addresses, geolocation cookies, and so on. Any two of these would be considered protected personal data. There is also a separate category of information beyond personal information that is protected under the GDPR with an additional layer of responsibility. That is what they classify as sensitive personal data. This category includes information such as: religion, race, cultural background, biometric data, fingerprints, retinal scans, genetic information, income, medical conditions, sexual orientation, political affiliation,

and so on. The GDPR requires explicit consent for this type of sensitive personal data.

2. An "identifiable natural person" is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
3. "Controller" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by EU or member-state law, the controller or the specific criteria for its nomination may be provided for by EU or member-state law.

THE RIGHT TO BE FORGOTTEN

One of the best-known requirements, largely because of US media coverage, is referred to as the "right to erasure," which is sometimes called the "right to be forgotten." It is found in Article 17. The UK Information Commissioner's Office provides this summary of the meaning of the right to erasure:[11]

11 Information Commissioner's Office of the United Kingdom, "Guide to the General Data Protection Regulation: Individual Rights," 2018, 1, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/

- The GDPR introduces a right for individuals to have personal data erased.
- Individuals can make a request for erasure verbally or in writing.
- Organizations have one month to respond to a request.
- The right is not absolute and only applies in certain circumstances.
- This right is not the only way in which the GDPR places an obligation on you to consider whether to delete personal data.

A data subject may have the right to erasure if:

- The personal data is no longer necessary for the purpose which the organization originally collected or processed it for.
- You are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent.
- You are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing.
- You are processing the personal data for direct marketing purposes and the individual objects to that processing.
- You have processed the personal data unlawfully (i.e., in breach of the lawfulness requirement of the first principle).

- You have to do it to comply with a legal obligation.
- You have processed the personal data to offer information society services to a child.

RIGHT TO RECTIFICATION

The purpose of the right to rectification is to empower individuals to correct inaccurate personal data or complete it if it is incomplete. A data subject can make a request for rectification either in writing or verbally. The data processor has one month to respond to the request. Unless there is a clear reason to deny the request, the supervisory authority expects the data controller to comply quickly and completely.

GDPR Article 16 explains the "right to rectification." The article states:

> The data subject shall have the right to obtain from the controller, without undue delay, the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

This right is built on the data controller's obligation of accuracy as specified in GDPR Article 5.1 (d):

> [Personal data shall be] accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

The GDPR does not define what "inaccurate data" means, but assume it will almost always side with the data subject. If the data is an opinion, then the data subject may not request to have it changed. But the record must clearly show it as an opinion and, where possible, must show whose opinion it is, since opinions are subjective by their nature.

What if the data is not an opinion but time is required to analyze the accuracy of the data? Article 18 provides some guidance and is entitled "Right to restriction of processing." Article 18.1 (a) states that processing should be restricted when:

> The accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data.

This means that the data processor should restrict processing of data being reviewed for accuracy. This applies whether or not a data subject has submitted a request for processing restriction.

Response to a request for rectification must be done within a month—sooner if possible. However, there are situations where more time can be requested. The GDPR will allow an extension of up to two months if the request is complex, or if you have received a considerable number of requests from the same data subject. If you intend to seek an extension, you must let the data subject know as quickly as possible (also within a month), and you must explain why.

WHAT ABOUT IDENTIFICATION?

It is understood that third parties might attempt to exercise rights made available under the GDPR when they should not have those rights. So a data processor is authorized to ask for clarifying identification where reasonable. The directive does not specifically address how the identification should be performed, but it is required where appropriate—as long as it is proportional to the data being processed.

If the data processor cannot appropriately identify the data subject, then the processor may not have to honour certain GDPR rights. In other words, if the data processor requires positive identification (due to the nature of the data) and such verification cannot be reasonably performed, then the data processor is exempt from the right to rectification and other similar rights.

CAN A FIRM REFUSE TO CORRECT DATA?

A firm can refuse a right to rectification request if it is unfounded or excessive. They can also refuse if the request is repetitive. The data processor may:

- Request a reasonable fee to deal with the request.
- Refuse to deal with the request.

The data processor should be prepared to justify their position. Any fee must be the administrative cost to comply with the request and must be reasonable. If you intend to charge a fee, you must respond within a month—sooner if possible—with that clarifying statement. If you intend to refuse to comply, you should:

- Be prepared to explain why you are refusing to act on the request.
- Be prepared for the data subject to file a complaint with the supervisory authorities.
- Be prepared that the data subject may seek to enforce their rights through judicial remedy.

RIGHT TO DATA PORTABILITY

The right to data portability enshrined in the GDPR requires that, when applicable, the data processor must provide the personal data to the data subject in a structured, commonly used, and machine-readable open

format that is not proprietary, such as TXT, RTF, or CSV. Machine-readable means information is structured to allow a software program to extract elements from the data, thus allowing other firms to import and process the data. In other words, not requiring manual entry or standardization.

The directive also requires that the data be provided free of charge. Individuals have the right to store their personal data on a private device for future personal use. They also have the right to have their data securely transmitted from one data controller to another as long as it is technically feasible and reasonable to do so. If the data subject has requested it and it is technically feasible, the source data controller may transmit the data directly to another data processor. The directive does not require that these types of facilities be implemented or maintained.

As always, the data processor has one month to comply with such requests.

TRANSPARENT COMMUNICATION

We live in a world where companies purposefully design complex user agreements to make interpretation complicated. When was the last time you read an end-user licence agreement before using software or an online service? The EU wants to ensure that personal data is

processed fairly and that data processors communicate transparently with people. They don't want data processors hiding behind incomprehensible user agreements.

The core concept is that the data processor should use clear and easy to understand language to explain what data will be stored and how it will be processed. You cannot hide this information in an eighty-page EULA or attempt to trick users into providing consent.

RIGHT OF ACCESS

The supervisory authorities understand that a data subject should have access to the information stored about them by a data processor so they can enforce their data-protection rights.

What rights does the data subject have? Below is a short list. The data subject has the right to:

- Confirmation of if and where the data controller is processing personal data related to the data subject, and an explanation of the purpose of processing.
- Explanation of whom (if applicable) the data is being shared with.
- Information about the length of time the data will be stored.

- Information that the data subject has the right to complain to the DPA.
- Request a copy of the data held by the data processor.

Similar to other sections, data controllers are allowed to charge a small fee for each request. This will help to dissuade people from making vexatious requests.

RIGHT TO OBJECT TO PROCESSING FOR THE PURPOSE OF DIRECT MARKETING

European citizens have the right to object to the processing of their personal data for direct marketing purposes. This is similar to "do not call" and anti-spam lists in Canada. The basic rule is that anyone can opt out of sharing their data for direct marketing use.

If the processing is necessary for the performance of a task carried out for reasons of public interest, the data processor may refuse the objection request.

RIGHT NOT TO BE EVALUATED ON THE BASIS OF AUTOMATED PROCESSING

People have the right not to be evaluated with an automated processing program. This means the data subject has the right not to be subject to a decision or decisions

based solely on an automated-processing facility that may significantly impact them in some material way.

This type of processing is permitted when authorized by law or if the data subject has explicitly consented, and only when the appropriate safeguards are in place. I see the addition of this right as a way to future-proof the GDPR. As more and more automation and machine-learning tools are used to process data, the GDPR says organizations must offer individuals a way to opt out and have their data evaluated by a human being, and not by a machine.

BEST PRACTICES WHEN COLLECTING DATA

This all leads to a few important questions. How can we lawfully process the personal data of European citizens in compliance with the GDPR? What are the conditions under which data can be processed? Below are a few guidelines.

First, you can always process personal data if you have obtained consent from the data subject. But you must clearly explain your intentions and methods. You must explain why you're collecting their personal data, how you're collecting it, what you're going to do with it, and how long you're going to keep it. If you do this, then you are allowed to process that person's data.

Second, you can also collect personal data in the perfor-

mance of a contract. If you enter into a transaction that involves signing a contract, and the contract clearly gives permission to collect and process data, then this is allowed as long as it is done lawfully and in accordance with the GDPR. For example, if a law states that you must keep seven years of tax records, then you have a lawful reason to keep that data for seven years.

The best practice is to err on the side of caution. Be extra cautious with personal data. Be extra transparent. The era of buying lists is over. The days of using one list to market a different product than what the individual consented to are over. If an individual doesn't give you consent, then you are obligated to delete their personal data.

Always think in terms of transparency and fairness under the new law. You will need to revalidate all the personal data that you have about a customer in the past. You're going to need to get consent again and make sure that the customer understands what personal data you have, why you have it, how long you're going to keep it, and what you're going to do with it.

THE EVALUATION PHASE BEGINS

There is no doubt the GDPR is going to be tough on companies. Most organizations have never designed their own systems to meet these types of requirements. It will

require massive changes in policy, process, software, and technology. Going forward, all systems must be designed or redesigned with privacy as the first priority—what we call privacy by design. If you have a system that has configuration options, the default configuration should always prioritize privacy.

Medium and large organizations will certainly comply with the GDPR. But the strict regulations may force some smaller companies to completely abandon operations in the European Union. Some firms will simply decide to no longer collect or process personal data for Europeans. How this affects the market and the availability of goods and services in Europe remains to be seen.

Complicating matters, there is a lot in the GDPR that is still unclear. Many of the finer points of the regulation need to be clarified. This will happen gradually over time, as organizations both try to comply with and test—or even avoid—the new regulation. It will be interesting to see which other countries jump on the GDPR bandwagon, especially a country like Canada, which prides itself on being a privacy-first country.

DO NOT WAIT

Taking a wait-and-see attitude and delaying to see how other companies are complying with the GDPR is a recipe

for disaster. Failing to take adequate steps to meet the regulatory requirements could be considered as negligence and can subject your organization to substantial fines. My recommendation is for companies to maximize their efforts to comply with the GDPR. If you get sanctioned under the new regulations, you will have to defend yourself and show the steps you've taken towards compliance.

For large companies and organizations, the path forward is clear. Comply. But the choice for smaller businesses is much less clear. Do you invest a lot of time and money on GDPR compliance so you can continue delivering services to Europeans? Or do you exit the EU and concentrate on growing your business elsewhere? These are difficult decisions that need to be made.

I believe the GDPR will evolve over time. I do not expect the existing laws will be the final format of these regulations. Looking five years out, the authorities will evaluate how companies are complying and how many have abandoned the EU because of the GDPR. If they see a sizable business shift out of the European market, then they may change some of the provisions. But for now, the law is clear and precise, and compliance is mandatory. Do not wait.

CONCLUSION

We've covered a wide range of topics in this book with a diverse group of contributors and perspectives. I want to leave you with a couple of final thoughts. First, cybersecurity is a journey, not a destination. There will never be a point at which a cybersecurity professional can say, "We are secure. We can relax. We're done." Even at the most secure organizations, with unlimited budgets, there is no time to relax and think you're completely safe when it comes to cyber. There will always be new threats and novel forms of attack.

Second, many cyber professionals have been educated and brought up in this industry believing that they can complete their work formulaically, choosing different tools off of a menu and following the standard prompts and protocols. That's a fallacy. The terrain changes, the road changes, there are landslides and tar spills, and plenty of roadkill along the way. There will be all sorts of threats and perils that you've never encountered before that can cause you to detour from your set plan. As cyber professionals, we're standing by the side of the road with our thumbs out, doing our best to get from A to B safely.

The type of individual who aspires to this field has to understand that not only is there no clear destination and no reliable map, there's no paved road. Nobody can accurately tell you what your journey is going to look like on any given day, in any given year, or in your entire career. So the cyber professional's mindset becomes one of the best weapons in this ongoing battle.

Finally, I would like to leave the reader with one softer piece of advice: have an open heart, an open mind, and empathy for your colleagues and coworkers. When you look at the impact of cyber, understand that it's the human impact of a technological concept. Recognize that in cybersecurity the inevitability of failure is a reality. Accept the fact that having humility is essential to being successful in this field—and almost any other field, but particularly in cyber. Maintain humility in the face of this arduous journey with no end, remain empathetic to those who join you on this journey, and have fun with it. Rather, have as much fun as you can when travelling the desolate, always challenging, never-ending, pothole-filled road of cybersecurity. It's a struggle, but you can indeed learn to celebrate your triumphs and enjoy yourself along the way.

Or you can just take the blue pill.

AJAY K. SOOD

ABOUT CLX FORUM

Cybersecurity Leadership Exchange Forum (CLX Forum) is a community of cybersecurity thought leaders whose primary objective is to create an environment where IT security professionals can network, learn, and exchange ideas.

For more information, please visit www.clxforum.org.