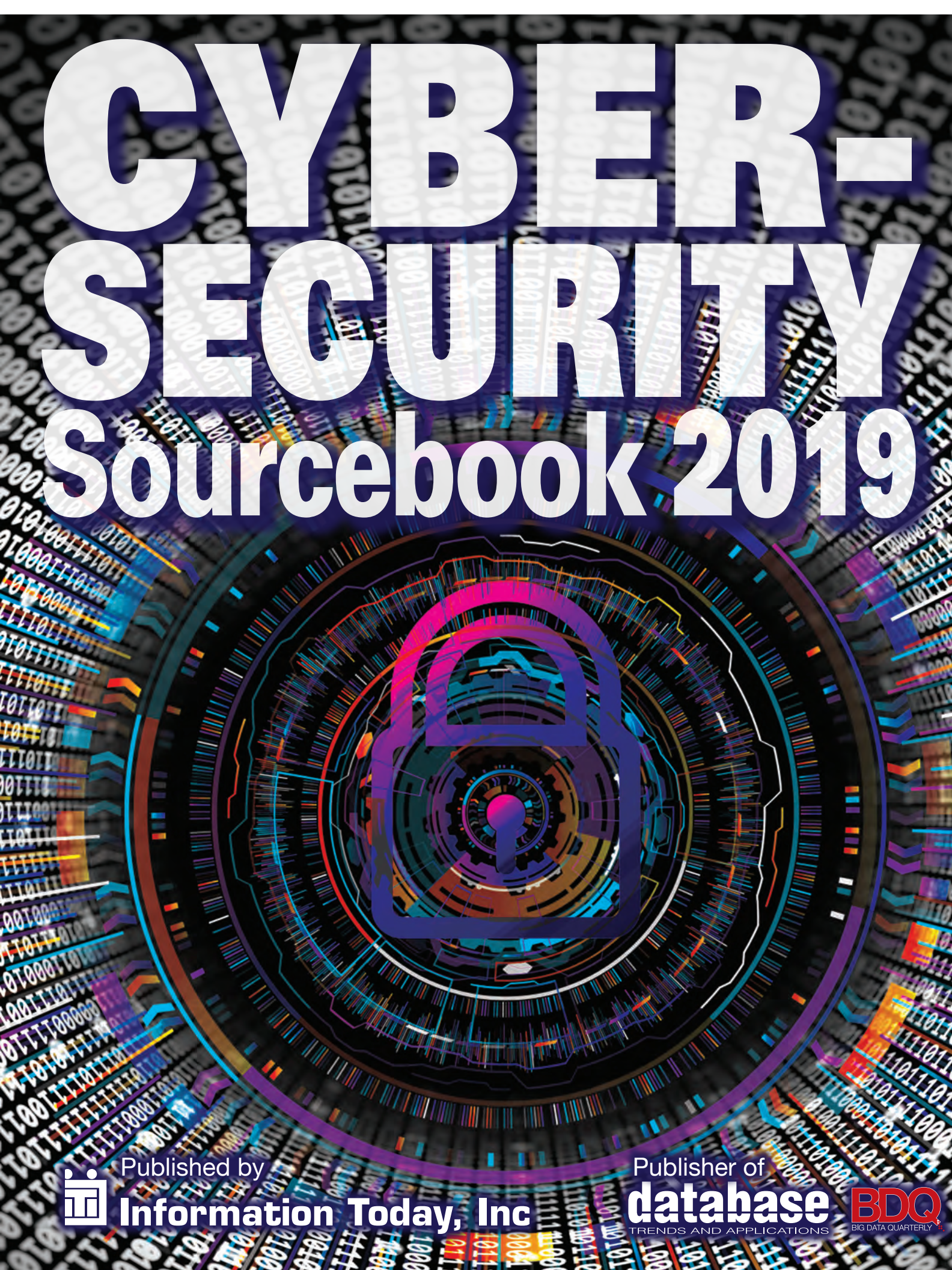
CYBER-SECURITY Sourcebook 2019



Published by
Information Today, Inc

Publisher of
database
TRENDS AND APPLICATIONS
BDQ
BIG DATA QUARTERLY

CYBERSECURITY SOURCEBOOK

From the publishers of database TRENDS AND APPLICATIONS BDQ BIG DATA QUARTERLY

PUBLISHED BY Unisphere Media—a Division of Information Today, Inc.
EDITORIAL & SALES OFFICE 121 Chanlon Road, New Providence, NJ 07974
CORPORATE HEADQUARTERS 143 Old Marlton Pike, Medford, NJ 08055

CYBERSECURITY SOURCEBOOK (ISBN: 2376-7383) is published annually by Information Today, Inc., 143 Old Marlton Pike, Medford, NJ 08055

POSTMASTER
Send all address changes to:
Cybersecurity Sourcebook, 143 Old Marlton Pike, Medford, NJ 08055

PRINTED IN THE UNITED STATES OF AMERICA

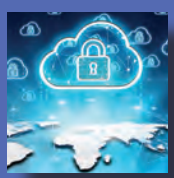
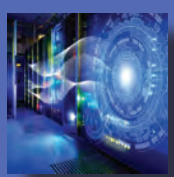
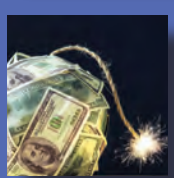
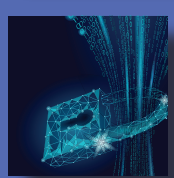
Cybersecurity Sourcebook is a resource for IT managers and professionals providing information on the enterprise and technology issues surrounding cybersecurity and the key challenges, opportunities, and technologies, as well as the approaches being evaluated, adopted, and bringing success. The *Cybersecurity Sourcebook* provides in-depth articles on the expanding range of cybersecurity technologies and best practices. Articles cover encryption and data masking, database auditing, database administration, IoT and connected devices, the business of data security, and regulatory compliance.

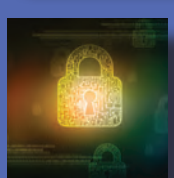
Information Today, Inc.

CYBERSECURITY SOURCEBOOK 2019

CONTENTS





editor's note

cybersecurity updates

Data Security Risks Climb

By Joyce Wells

The pressure on companies to protect data continues to rise. Increasingly stringent data privacy regulations coupled with the lower public tolerance for data mishandling, are making companies even more concerned about improving their governance postures and thwarting cyber-risk. The issues are only becoming more challenging with the overlapping trends of data volumes exploding, data being collected from more disparate sources, and data no longer being stored centrally, but instead in a combination of on-premise, cloud, and hybrid scenarios.

With the growing awareness of the risks associated with data loss and misuse, there are now tough data breach and notification laws such as the EU's GDPR, Canada's Personal Information Protection and Electronic Documents Act, and the California Consumer Privacy Act of 2018, in addition to industry mandates that have practically become household names such as HIPAA, PCI-DSS, and SOX.

According to IBM's "2018 Cost of a Data Breach Study," conducted by Ponemon, data breaches are becoming more costly to companies, and are resulting in more data being lost or stolen.

The 2018 study found that the average total cost of a data breach rose from $3.62 million to $3.86 million, a rise of 6.4% over the previous year; and the average cost for each lost record rose from $141 to $148, an increase of 4.8%. The average size of a data breach had also increased by 2.2%, according to the research.

The IBM survey identified the relationship between the speed of identifying a breach and the cost of the breach. According to the study, the mean time to identify a breach was 197 days, and the mean time to contain a breach was 69 days. Companies that were able to contain a breach in 30 days or less saved more than $1 million compared to those that took more than 30 days to resolve it.

New Dell EMC research has also revealed that while organizations have a strong recognition of the value of their data, they are nonetheless struggling with data protection, in part due to the sheer volume. The third "Global Data Protection Index" noted that on average, organizations were managing 9.7PB of data in 2018, an increase of 569% compared to the 1.45PB managed in 2016. Of those surveyed, 76% experienced a disruption in the prior 12 months, and 27% experienced irreparable data loss. While more than a third (35%) of the respondents were very confident that their data protection infrastructure complies with regulations, only 16% said they anticipate that their data protection solutions will meet all future challenges.

But despite the challenges of doing so, focusing on data security is critical to business success, another study points out. According to a report released by CA Technologies in July 2018, nearly half (48%) of consumers reported that they use or have used services offered by organizations that were involved in a publicly disclosed data breach and, of those, 48% stopped using the services of an organization due to a breach. CA's "Global State of Digital Trust Survey and Index 2018," conducted by Frost & Sullivan, identified a "significant gap" between how organizations see their data governance responsibilities and consumers' views on how they want and expect their data to be protected.

On the following pages in *DBTA*'s annual *Cyber Security Sourcebook*, industry experts shed light on the ways the data risk landscape is being reshaped by new threats and identify the proactive measures that organizations should take to safeguard their data. As regulatory requirements increase, the potential fines for non-compliance grow more onerous, and consumers' and business partners' tolerance for data mishandling declines, it is incumbent on all companies collecting and storing data to take a more aggressive position on data security. This includes oversight of trusted users' data access, taking steps to block attacks by hackers, and careful management of data as it travels both throughout an enterprise and between partners. ■

IRI
Total Data Management

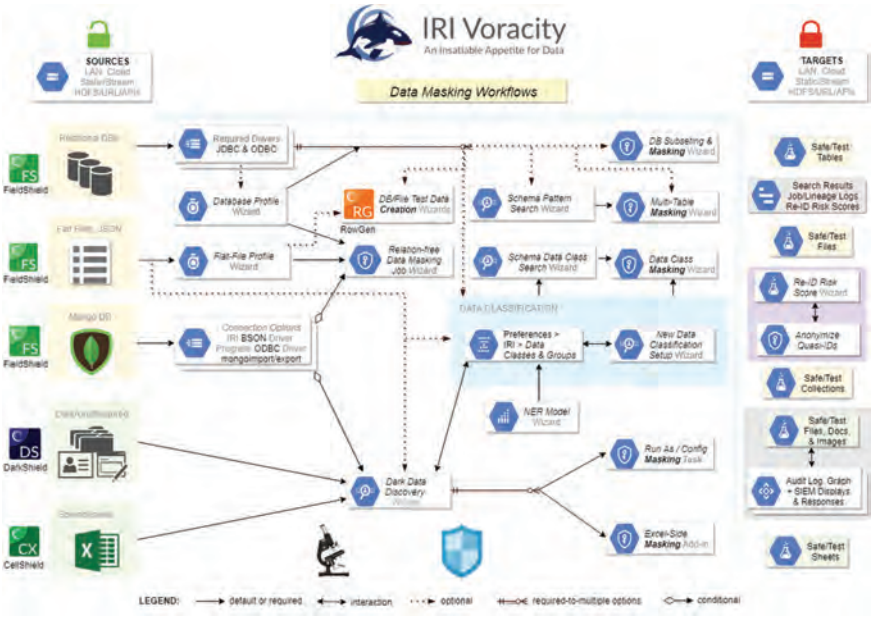
Discover, Classify and Mask PII in Structured and Unstructured Sources

In the last issue of *CyberSecurity Sourcebook*, IRI defined the term 'Startpoint Security' to encompass nine data-centric security concepts:

1. Permission & Disclosure—authorizing you to store submitted PII via user agreement
2. Discovery & Classification—finding and cataloging PII to find and mask it consistently
3. Data Masking—de-identifying PII via encryption, redaction, pseudonymization, etc.
4. IAM & RBAC—managing access to sources, (un)masking jobs, programs, and logs
5. Data & Metadata Lineage—saving and analyzing changes to data and masking jobs
6. Latency—architecting, configuring and running static or dynamic data masking jobs
7. Risk Scoring—measuring the statistical likelihood of re-identification (e.g., for HIPAA & FERPA)
8. Audit Logs—seeing or querying who did what, and who saw what, when, and where
9. Assessment & Insurance—conducting expert procedural, statistical, and legal reviews

These activities can complement and be used in conjunction with end-point security approaches to harden vulnerable data targets against hackers, insider threats or breaches, and to comply with both U.S. and international data privacy laws.

IRI currently offers three interrelated data masking products that satisfy the bulk of these requirements based on the data sources involved:



- **FieldShield**—RDB tables and flat files/streams, plus MongoDB and JSON sources
- **CellShield EE**—MS Excel spreadsheets 2010 and later, in local/LAN/cloud folders
- **DarkShield**—unstructured text files, documents and image files in several formats and locations

All, plus RowGen for test data creation, are front-ended in the same Eclipse IDE called IRI Workbench, and all their search results and masking logs can be exported to SIEM tools like Splunk Enterprise Security.

The schematic above diagrams the typical flow of activity through these products and serves as a how-to template for solution design and implementation.

These products also belong to the IRI Data Protector suite, and are included components of the IRI Voracity data management platform. You can find Voracity in recent DBTA special reports and buyers' guides covering big data, data integration and governance, data lakes, and cybersecurity, or at iri.com/voracity.

If you would like a white paper on the case for data masking, or require information on the IRI technology or services that drive these results, see iri.com/solutions/data-masking or contact info@iri.com. ■

IRI, THE COSORT COMPANY
www.iri.com
+1.321.777.8889
info@iri.com

Information Governance and Data Management Initiatives:

Are You Still Waiting to See What the Future Brings?

By Linda Sharp

Over the past several years, we have seen a tremendous amount of pressure from consumers (and now regulators) regarding how organizations manage content, especially when that content contains information about employees, consumers, and any number of other individuals whose data has made its way into enterprise data stores. Although the enactment of the EU's General Data Protection Regulation (GDPR) in May 2018 seemed to monopolize public discussion, we have seen a multitude of other newsworthy moments since then.

In fact, during 2018, we started to see organizations targeted for inappropriately managing personal data. According to CNET, on the first day that GDPR went into effect, as anticipated, the likes of Google and Facebook (and its subsidiaries) were hit with a number of claims that could yield $9.3 billion in fines. Regulators around the globe are taking data privacy seriously, as evidenced by the vast array of new privacy requirements.

In the past year:

- California joined the privacy conversation with its proposed California Consumer Privacy Act (CCPA), due to take effect January of 2020. (Don't forget the look back provisions!)
- India initiated its efforts with its Personal Data Protection Bill 2018.
- Japan furthered its efforts with regard to privacy and negotiated terms with the EU regarding cross-border data transfers.
- On August 14, 2018, Brazil executed its General Data Protection Law and although it largely follows GDPR it won't go into effect until early 2020.
- Canada amended its Personal Information Protection and Electronic Documents Act (PIPEDA) of 2000 in November 2018 to include mandatory data breach notification and record-keeping laws.
- China implemented the final version of The Standardization Administration of China's privacy bill in January 2018 which went into effect in May 2018 and is widely regarded as more rigid than GDPR.
- The U.S. Congress submitted proposed bills which put a Federal Privacy Policy on our radar for 2019.

The bottom line is this: People everywhere are getting on board with increased privacy measures. We cannot continue to manage data with the "same old, same old" mentality. Far too many times, I've heard middle management comment that GDPR doesn't apply to them or that they just won't land on the regulators' priority list. While that argument has its points, privacy regulation has expanded well beyond the scope of GDPR. California, home of the new CCPA, is the world's fifth largest economy, and the number of countries with their own specific and unavoidable regulations is constantly growing. One of the myriad of privacy regulations is going to apply to you, so that argument no longer passes muster. In fact,

it is time to understand what your organization is doing with data stored in your environment, where it came from, and why you have it.

The Growing Data Universe

As we look at our crystal ball and consider what 2019 might bring to this topic, one can only wonder if this ever-increasing deluge of data will stop to let us get a handle on what we already have. For better or worse, it probably won't. With the size of the digital universe projected to double every 2 years, it is imperative that we gain control of these mounting volumes of data immediately, or else they will continue to grow unmanaged and increasingly create greater risk to organizations.

This daunting task can only be effectively accomplished by implementing processes, policies, and technologies that manage data at the point of creation and regardless of where it is stored. Unfortunately, focusing on data on a "go-forward" basis alone won't be enough. In order to achieve efficient data management at scale, one must understand the various available technologies' ability to scale to meet specific needs. This means assessing the various offerings' ability to manage and ingest new data as it is created while simultaneously ingesting and classifying the content that has lived in data stores for potentially years. It further dictates a process by which expired data may be defensibly disposed from both data stores.

The Hidden Value of Data Management

While data management initiatives doubtlessly have regulatory relevance, they can also provide a tangible ROI through improving the enterprise's data analytics capabilities. Organizations seeking competitive advantage believe that there is "gold in them hills" and are looking at ways to leverage their data beyond compliance, management, and disposition. By applying modern technologies and thoughtful processes, it's possible to mine your organization's content—structured and unstructured—and repurpose it to gain real business value.

It has become common knowledge that our loyal and long-term baby boomer employees are retiring at breakneck speeds while their positions are being replaced by millennials. Evidence has shown that millennials are prone to rotate jobs every year or so, thus, creating business content, participating on teams that are creating products, and attending any number of meetings, then leaving your employment. This is one area where responsible data management can help your organization.

*With the size of the digital universe **projected to double** every 2 years, it is imperative that we gain control of these mounting volumes of data immediately, or else they will continue to **grow unmanaged** and increasingly creating greater risk to organizations.*

The days of bellowing down the hall to ask a long-term employee who worked on a specific initiative for their thoughts or recollections are over. Millennials may move on to the next employer before their seat even begins to get warm. If you do not take control over your data, you are limiting the ability to identify work product not only created by your baby boomers but also by various millennials that worked for you, including the meetings they attended, and the data they created or came in contact with. As we look into the crystal ball, I speculate that if we fail to implement the requisite processes and technology, we will find it is relatively impossible to reasonably defend or prosecute an IP claim, or defend a regulatory or civil investigation, especially where the alleged acts are from a millennial that has moved on to another employer.

Data Management Comes First

Numerous organizational initiatives are always jockeying for a limited budget—that will never change. But as of 2019, priorities have changed, and data management is now topping the list. Arguing that there is no budget to implement a data management initiative will fall on deaf ears when executives are faced with the very real risk of being hauled before regulators or international courts to explain why sound data management practices were not implemented. Members of the executive team can no longer relegate such important decisions to middle management while at the same time invoking budget restrictions, thus tying their hands from implementing strong policies and practices.

The only way to resolve this issue is to truly evaluate your organization's data: What data do you maintain in your existing data stores? How is it collected? What legitimate business purpose is this information being stored for? What business value could be mined from it? What disposition policies should exist? And, most importantly, how are you going to actually carry everything out?

As many organizations run statistical models to define their risk, others merely flip a coin as they attempt to define the likelihood that they might get hit with a regulatory investigation—but at what cost to the organization? It isn't just about calculating a hard financial ROI on the risk of getting caught, many other factors must be calculated into the equation. There are other penalties for improperly managing data, for example: loss of consumer confidence, ineffective business decisions, lost productivity as employees waste time looking for work product that was previously created, and lost access to the institutional knowledge that was created by employees long gone.

The bottom line is this: The clock is ticking. Will you find a way to leverage your institutional knowledge, or will you continue to allow it to sit in storage facilities that are nothing more than black holes? ■

Linda Sharp, Esq., MBA, is the associate general counsel for ZL Technologies (http://zlti.com). Her responsibilities include corporate legal matters and related legal product initiatives. Prior to joining ZL, Sharp consulted with Fortune 500 companies and Top 200 law firms on federal investigations and large litigation matters. She writes and speaks regularly on the subjects of e-discovery, records management, and information governance. She is an expert in her field, with membership in the OLP Advisory Board, and a chair position with the ACC New In-House Committee.

Principles of Database Security Planning

By Andrew C. Herlands

As the volume of digital information being produced across industries grows at record rates, databases are becoming more integral to organizations than ever before. These data stores contain the lifeblood of an organization and the sensitive information within them must be protected from improper access and breaches, which continue to rise in frequency. In 2017, there were more than 1,500 data breaches reported in the U.S. alone—nearly a 45% increase year-over-year—and according to the Ponemon Institute, the average cost of a data breach rose to $3.86 million.

Cybercriminals will use every tool in their bag to try to gain access to an organization's sensitive data. This might include leveraging social engineering, phishing emails, malware, security exploits, compromised endpoints and user credentials, or unpatched vulnerabilities, to name a few. Yet, even as threats increase, at many organizations, database security is given less importance than perimeter defenses. Organizations often reinforce their network perimeters through firewalls and other security measures, but overlook the databases themselves.

To reduce the risk of compromise and maintain compliance with numerous data security regulations, organizations must extend data protection measures down to the database level and implement a robust, database-specific security plan. An effective database security program requires commitment and discipline across the organization. Policies must be established, standard configurations must be reviewed, and databases must be continuously monitored for compliance. Most importantly, an operational methodology consisting of technology, people, and processes must be documented and institutionalized.

The following are some best practices for creating your database security program.

Begin with a Thorough Assessment

The first step in establishing a strong database security program is to assess the current state of operations and ensure you have an accurate database inventory. Determine who owns the rogue databases that will likely be uncovered during the assessment and classify databases that are mission-critical to the organization. The assessment should also cover policy management, vulnerability management, and access management in order to identify any issues or areas that need immediate remediation. The assessment phase is necessary for establishing a baseline of known database configurations and user privileges. Prioritize and fix the most critical issues first, then after working through the list, retest to document remediation progress.

A common misstep and a sure path to spending more than necessary on a database security program is bypassing the assessment phase and installing database activity monitoring (DAM) without first understanding how critical elements integrate. Deploying DAM before conducting due diligence will often result in a solution that monitors and collects everything, generating overwhelming reports, logs of indeterminate data, and a flurry of false positive/negative alerts, which then lead to resource drain and frustration.

Define Security Standards and Compliance Policies

Policy management is a continuous process. Without defined polices and standards to conform to, an organization cannot measure compliance or progress against benchmarks. In many instances, organizations develop robust corporate policies for protecting data as it traverses the network but fail to map those policies back to the databases themselves. When security weaknesses are remediated, it is usually a reaction to an incident rather than a proactive response to a standard or policy. A good rule of thumb is to review and update your policies after patching vulnerabilities or installing new versions of software, to ensure they account for the latest security configurations and settings.

When defining standards and policies, make sure to have answers for the following:

- What is the frequency of policy updates?
- Who is the person (or persons) responsible for updating policies?
- What are the triggers for policy change?
- What is the approval process for a policy change?

Conduct Vulnerability and Configuration Audits

Regardless of the industry in which they operate, most organizations need to demonstrate compliance with more than one set of business, security, or regulatory policies. Because databases are often an organization's largest repository of sensitive data, they typically fall within the scope of regulatory compliance checks and the inevitable IT audit. IT security and compliance teams will often partner with DBAs to ensure database security configurations meet the requirements of any number of industry standards and regulations, such as: Sarbanes-Oxley, the Payment Card Industry Data Security Standard (PCI DSS), the Federal Information Security Management Act (FISMA), the EU's General Data Protection Regulation (GDPR), and the Health Insurance Portability and Accountability Act (HIPAA).

To demonstrate effective controls surrounding sensitive data, organizations will need to run a baseline audit and establish a practice of continuous assessment to ensure issues are remediated in a timely manner and progress is tracked against the organization's standards. An exemplary model to follow is the Continuous Diagnostics and Mitigation (CDM) mandate developed by the Department of Homeland Security (DHS) for ensuring database vulnerability compliancy.

DBAs should also ensure they stay current on database versions and patches as soon as they become available or, at the very least, prioritize patches based on criticality. Leverage the built-in security protocols and controls of your database, unless there is a valid reason to keep them off. Delete or disable any unnecessary or unused features or services but be sure to document all exceptions before the auditor shows up. Misconfigured database configurations and security controls can inadvertently lead to system compromise, so test and retest to be sure you have a handle on everything, especially after applying a patch.

Identify Users with Excessive Privileges

One particularly challenging question for many organizations is, "Who has access to my sensitive data?" Overprivileged user accounts can be leveraged to gain unauthorized data or systems access, and even to erase evidence along the way. Many database scanning technologies can not only identify vulnerabilities and misconfigurations, but also users, roles, and privileges. The only way to establish meaningful controls that track how users interact with data, or to capture an audit trail for use in a breach investigation, is to know who has access to what data, and why, when, and how they've been granted that access.

Frequently review not only who has administrative access, but also that database users have appropriate and minimum privileges necessary to perform their work (the Principle of Least Privilege). While enforcing segregation of duties in the database may seem to be a daunting and manually intensive job, automating rights review assessments can save upward of 80 man-hours per database instance.

Detect, Alert, and Respond to Policy Violations in Real Time

After conducting a thorough discovery and assessment of databases and implementing best practices in access control, organizations may want to consider implementing a real-time DAM solution to keep the database security plan in line. Monitoring gives security teams the needed up-to-the-second intelligence to take prompt action such as terminating user sessions or locking down accounts when violations occur or threats are perceived. Further, monitoring privileged user activity helps ensure that authorized activities are securely tracked, unauthorized behavior is not occurring, and ongoing monitoring of the database helps identify new avenues of attack.

Keep in mind that you don't need to monitor everything, or you will find yourself constantly searching for the needle in the haystack. Instead, determine what is most important for your business to monitor—such as critical databases, sensitive database objects, highly privileged accounts, policy violations, access during off-hours from unauthorized hosts, or from services accounts reserved for recurring tasks or system maintenance jobs, etc. Be prescriptive in your monitoring policy.

Parting Advice

By following these steps, you will be well on your way to establishing a strong database security program. There are, however, a few remaining best practices that can help take your program to the next level. Consider encrypting data at rest, in use, and in motion. Seek out guidance and use security checklists and frameworks from government agencies and industry standards bodies such as the Center for Internet Security (CIS), the Defense Information Systems Agency's Security Technical Implementation Guide (DISA-STIG), and others.

Finally, hack yourself. It is the only way to know what the auditor—or an attacker—will find, before they show up. If you don't have the skills or time to do this yourself, consider working with a security company that offers managed database scanning. After implementing the above advice, "rinse and repeat" to ensure your database security program is repeatable and measurable. Make sure your reporting and analytics produce a clear and accurate picture of your database security posture, as well as the progress made since your last report.

Establishing or operationalizing a database security program can be daunting and resource-intensive. If your organization is just getting started, or if it doesn't have the necessary in-house expertise, consider bringing in experts to help establish a plan and build a program suited to your goals, and integrate that plan with your existing security solutions and teams. By incorporating database security planning into your larger IT security strategy, you will help your organization better protect its most valuable data assets and seal a serious gap that is far too often exploited by cybercriminals. ■

Andrew C. Herlands is VP, Global Systems Engineering, at Trustwave (www.trustwave.com), with overall operational management responsibilities for the global pre-sales teams. He brings more than 2 decades of security industry knowledge to Trustwave. Prior to joining Trustwave, Herlands was the chief security officer and VP WW Services at Application Security, Inc., which was acquired by Trustwave in November 2013.

Defending the Enterprise From the Coming Wave of Ransomware Attacks

By Sash Sunkara

Ransomware attacks faded from the headlines after the notorious WannaCry outbreak in 2017 and the frequency of attacks declined in 2018. And yet, with ransomware threats seemingly in the rearview mirror, cybersecurity experts and the Information Security Forum's 2018 Global Security Threat Outlook are suddenly forecasting a major resurgence of ransomware this year.

Why? Because ransomware never went away—it simply changed.

In the past, threat actors targeted any vulnerable computer they could find. Now, they're targeting enterprise networks with cryptojacking malware. And with 80% of enterprise workloads migrating to the cloud by 2020, that means the cloud is set to become the next battleground in enterprise cybersecurity.

Ransomware: What to Expect in 2019

Ransomware poses a serious threat to enterprise security. According to FBI estimates, ransomware payments in the U.S. have totaled $1 billion or more in some years—a figure we could easily surpass in 2019 if cybersecurity forecasts are accurate.

Many, if not most, of this year's ransomware attacks will occur in the cloud. But whether your organization's data infrastructure exists in the cloud or on-premise, it's important to understand the ransomware threat and how your enterprise should respond to it.

Every enterprise is vulnerable to the next wave of ransomware attacks. In 2019, many enterprises were lulled into a false sense of security about ransomware. But in the current environment, complacency may be fatal because the next wave of attacks will target enterprise networks. If you don't think your enterprise is a target, you probably haven't implemented systems and processes to counter ransomware threats. The time to start thinking about ransomware is now—before your business comes under attack.

When it comes to ransomware, the worst is yet to come. Although WannaCry and other ransomware attacks were devastating, they pale in comparison to the potential attacks that lie ahead. Threat actors in the ransomware arena are growing more aggressive, requiring enterprises to respond with sophisticated solutions. Temporary fixes won't cut it in 2019. To protect your organization, you'll need a more comprehensive security strategy.

The cloud is the new ground zero for ransomware attacks. Enterprise cloud environments feature the same level of security as data centers. In many cases, cloud environments are more secure. However, it's important to recognize that cloud environments face the same threats as data centers. As ransomware attacks evolve, cloud providers will need to ramp up the sophistication of their security measures or leave countless enterprises exposed to cyberdisasters.

Enterprise IT shares responsibility for security with cloud service providers. The cloud allows enterprises to offload the burdens of managing a data center or network. But that doesn't mean enterprises can completely outsource security to cloud services providers, especially given the seriousness of the ransomware threat in 2019. Instead, security must be the shared responsibility of the cloud provider and enterprise IT. While cloud providers are responsible for supplying the necessary architecture, enterprise IT shoulders responsibility for ensuring that the right measures are in place to protect the business from ransomware and other threats.

Some enterprises won't know they've been hit until it's too late. Ransomware actors rely on stealth—they often allow an attack to go on for weeks or even months before they notify their victims. Enterprises that believe they will immediately recognize an attack are mistaken and highly vulnerable to significant data loss. To mitigate risk and reduce exposure, intrusion detection and protection solutions are prerequisites for this wave of ransomware attacks.

False positives are a problem for many enterprises. Just as with the little boy who cried wolf, false positives breed complacency. If threat detection solutions routinely flag false threats, enterprise IT teams are more likely to overlook genuine threats when they occur, ramping up the organization's risk exposure. Although false positives happen, enterprises will need to focus on the accuracy of security solutions to defend against attacks.

Untested disaster recovery plans will fail. The mere presence of backup and recovery plans isn't enough. Enterprises that fail to routinely test and validate for their environments leave themselves vulnerable to ransomware attacks. By proactively testing and determining your responses to all possible scenarios, you can minimize the impact of potential attacks on your business and its bottom line.

Cloud segmentation is a factor. Cloud segmentation will play a key role in enterprise security. Although a robust monitoring program is important, enterprises will need to evaluate their cloud segmentation strategies to withstand an attack. In the unfortunate event of a breach, the enterprise needs to know that a ransomware infection won't infect its entire cloud environment.

The odds are stacked against your enterprise. A successful ransomware attack can yield a serious payday for hackers. So, not surprisingly, threat actors are highly motivated to not only step up their attacks on enterprises, but to constantly adapt their tactics. Whether you know it or not, the probability of an attack on your enterprise is on the rise and the odds will be stacked against your organization if you don't have a security strategy in place.

Savvy enterprises are nailing the basics. The good news is that a security strategy against ransomware attacks is achievable for nearly all enterprises. In 2019, enterprises that master the basics will be in a better position than those that refuse to take any additional security measures. Start by investing in intrusion detection and protection technology that alerts you when an abnormal number of files are updated, and provides multiple recovery checkpoints with different retention points.

Next Steps in Enterprise Security for Ransomware

The ransomware threat for enterprises in 2019 is very real and it's important to act as quickly as possible to protect your organization. The cloud-based nature of the next wave of attacks means that enterprises must evaluate their cloud strategies to adequately defend against threat actors.

Right out of the gate, enterprises should consider a multi-cloud strategy. In addition to enabling your organization to avoid vendor lock-in, a multi-cloud approach mitigates the impact of a breach originating from any given vendor. In general, a multi-cloud strategy is more cost-effective, scalable, and secure than relying on a single cloud services provider.

Similarly, it may be useful to perform a platform audit. Enterprises frequently use comprehensive platform audits to highlight areas for cost savings. But they can also help determine the enterprise's security readiness for ransomware and other cyberthreats. At a minimum, a platform audit will clarify areas where enterprise IT needs to take action.

Finally, it's essential to manage your organization's cloud platforms effectively. A multi-cloud strategy and hybrid cloud architecture can present significant management challenges, so you may need to engage a third party to help manage your platforms and eliminate gaps in security.

The possibility of a successful ransomware attack is a terrifying thought for leaders of any organization. Although we're currently facing an elevated risk from ransomware, your enterprise is far from helpless. By understanding the ransomware threat and taking the appropriate steps now, you can insulate your business from the impact of an event in 2019 and beyond. ■

Sash Sunkara, co-founder and CEO of RackWare (www.rackwareinc.com), is a technology executive with extensive expertise in solutions for data centers. Before RackWare, Sunkara served as VP of program management at Brocade Communications and VP of marketing for QLogic's Network Solutions Division. Sunkara also founded 3Leaf Systems, a venture-backed server virtualization company.

Cloud in the Shadows

By Bob Post

Done properly, migrating to the cloud takes skilled staff to re-architect systems and applications, significant planning to ensure a successful migration, and a well-executed security strategy. However, many enterprises started migrating to the cloud sooner (or migrated faster) than they even realized—through a rogue marketing department deploying a cloud lead tracking application, a finance group that stood up a cloud-based accounting service—or others that IT may not have vetted, secured, procured, and continuously monitored. Most enterprises have scores of these "shadow cloud" applications deployed with little-to-no planning, strategy, or skilled technical staff involved, posing risk to the organization.

In many ways, this phenomenon is easy to understand: Data is the lifeblood of the modern enterprise. Recent studies have stated that 4% of all jobs in the U.S. and 5% of our national output come from the contributions data makes to the economy. Deriving this potential value from data takes computing power. Cloud computing with its service on demand and scalability has become an attractive option for enterprises. In making the transition to cloud environments, leading enterprises take the time to develop migration strategies to deal with the complexity and risk associated with the transition. They look at workloads, deter-

mine the applicability of that workload to the cloud, prioritize projects, and execute against their chosen strategy.

Unfortunately, that all takes time. And if a business unit's needs aren't high on the priority list, that department will often act on its own so it can quickly derive value from the data and show business results from their efforts. The ease of purchasing cloud services enables business units to acquire cloud services without going through normal procurement channels.

The result can be shadow cloud run amok. Your enterprise's transition to cloud services may have happened without you even knowing it (or happened faster, or more aggressively). Valuable data may be leaving your environment without your knowledge of where it's going and how it's getting there. If this were cash (and in today's world, data is in many ways equivalent to dollars), what would the chief financial officer do?

The shadow cloud poses significant risks to the enterprise. First, you no longer know where your data resides. Second, if a shadow cloud is made up of consumer-grade solutions, the consumer-grade SaaS solutions often don't offer the same level of security and protection that enterprise-grade solutions do.

Another significant consideration is that cloud security is built around a shared responsibility model. The cloud provider is responsible for certain security features and the customer is responsible for others. Without the support from your enterprise's security team, who is fulfilling the customer responsibilities (and how are they being fulfilled)?

These risks have potential regulatory, financial, and operational impacts. From a regulatory standpoint, you may no longer be able to fully identify where protected information such as personally identifiable information or electronic personal health information is stored or transmitted. If a data leak or breach occurs, there could be significant regulatory penalties that you thought you had already mitigated in your enterprise.

In addition to working to implement appropriate security controls within your enterprise, you also may have sought to transfer some risk by purchasing cyber-risk insurance—which brings us to the financial impact. When you apply for cyber-risk insurance, there is generally a form to fill out that describes any sensitive data you may have, the systems in which it is located, and how it is protected. If a data breach occurs and the data is not where you say it is or protected in an appropriate manner, it is entirely possible that any claim you submit may be denied.

*If you have **cyber-risk insurance**, and data is not where you say it is or protected in an appropriate manner, it is entirely possible that any claim you submit **may be denied**.*

Finally, there is the operational impact to consider. If the data contained in the shadow cloud were unavailable or somehow corrupted, what affect would that have on your business? Events that could cause the data to be unavailable range from the cloud provider going out of business to a ransomware attack that locks up your data. When the business units purchase unauthorized cloud services, they often fail to ask exhaustive questions about backups and disaster recovery procedures.

With the risks and potential impact high, what is a chief data officer to do? Here are some tips:

• **Discovery**—The first step is to use a tool to discover what shadow cloud applications are being run in your enterprise. Tools include the Microsoft Office 365 Productivity App Discovery Tool (requires a subscription to Advanced Security Management); a feature set on many cloud access security broker solutions such as Bitglass' Zero-day Unmanaged App Control; or a service such as Cisco's Cloud Consumption as a Service.

• **Assessment**—Once identified, talk to the users of the shadow cloud to determine the business need that is being met by the unauthorized services.

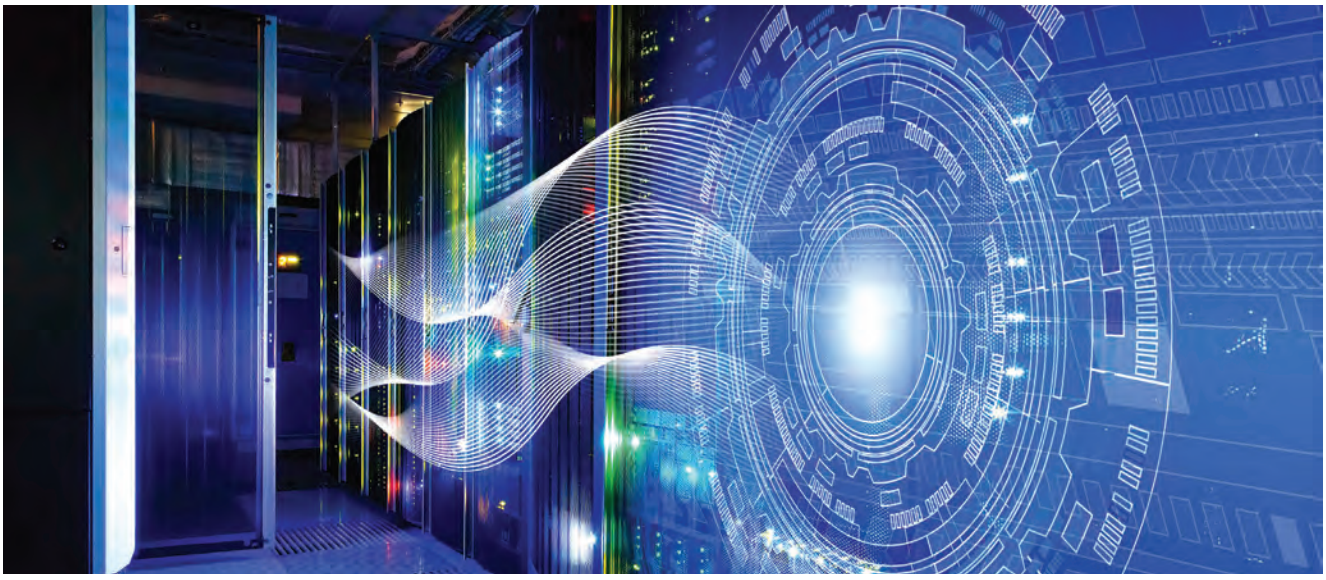
• **Analysis**—If a legitimate business need is being met with a particular shadow cloud service, identify whether there is an enterprise-grade service that will meet the same business need and provide the needed security features. If so, arrange to purchase the enterprise-grade version and migrate users to the authorized service.

• **Prevention**—If there isn't a valid business need, there isn't an enterprise-grade version, or the risk is deemed to be too high, work with the network team to block access to that service.

• **Educate**—Ensure everyone in your organization understands the value of data and what must be done to protect it. Individuals generally don't break the rules without reason; they most likely have a job to do and seek the most efficient way to accomplish it. Teach them the risks inherent in unmonitored, unvetted cloud applications and the appropriate processes they should follow if they wish to use a cloud service (or any new enterprise application).

In a fast-paced business environment, dealing with the shadow cloud can be challenging. Even with a well-thought-out migration plan, there will always be individuals who want to take advantage of the newest offerings to improve their personal and company performance. If it is thought of at all, the downside risk is minimized. As a community, we need to recognize this and rein in the shadow cloud. ■

Bob Post is the managing principal of at Coalfire (www.coalfire.com), a provider of cybersecurity advisory and assessment services.



Five Trends Driving Security in the Era of Emerging Tech

By Mark Sangster

Nearly every week of 2018 featured headlines of a new cyberattack on companies that people trust with their data, such as Marriott and Facebook. In years past, the biggest concern for companies was being hit with hefty fines, but now, they risk reputation damage if they breach compliance mandates and regulations when they are attacked.

Due to attack pervasiveness and cost, cyber-risk is now a business issue with board-level visibility and increasing spending for preventative services. According to research from eSentire, cybersecurity is no longer only on the minds of IT departments. Today, 60% of business leaders and board members expect that an attack will hit in the next 2–5 years. While the executive team knows cybersecurity should be a major concern, only 30% are confident their business will avoid a major security event within the next 2 years.

Cybersecurity used to be a part of the business related only to the IT department and the CIO. The adage, "the chief intelligence security officer (CISO) is the least interesting person to the board, until they are the most important person," is no longer true. The research shows that, as attacks have grown, 50% of boards are very familiar with security budget, overall strategy, policies, and technologies, and currently review present-day security and privacy risks. Through this familiarity, 77% of CEOs and boards are optimistic about their firms' ability to cope with a breach, but only 33% are confident that high value assets are adequately protected.

Additionally, there's a cybersecurity preparedness paradox between the CEO and board and the tech team. Business leaders are overconfident in their ability to manage a major security breach, but IT departments aren't as optimistic: Tech leaders are 20% more likely to predict an attack and are 10% less optimistic than business peers in their organization's preparedness.

As threats grow more pervasive, there's a wild card at play: emerging tech. These emerging technologies, such as AI, are evolving at a rate with which IT departments struggle to keep pace. At the same time, IT departments are held accountable for business disruption due to expanded threat surfaces that are created by these new technologies in tandem with increasingly sophisticated attacks. As these technologies continue to be adopted by organizations at a rapid rate, they create new security risks because organizations cannot put measures in place to prevent breaches from happening. These emerging technologies have all grabbed headlines for making business-critical operations more seamless, but the risks associated with these technologies is expected to grow. It is the CISO's job to keep the C-suite informed of and prepared for security threats in the era of emerging tech.

Risks Associated with AI

Companies across industries are turning to AI to improve customer experiences, automate work processes, and provide analysis. In fact, 44% of respondents indicate that they have adopted AI to help streamline business operations. The research found that the risks posed by the adoption of AI doubles over the next 3 years. This is due to:

- **AI creating more false positives:** Organizations continue to adopt AI to identify

security issues, but the result has been an increase in alerts that security teams must add to workloads that are already maxed out. It is simple to create models that detect potential threats and, on the surface, it appears that these models provide additional security. However, the models generate more false positives that prevent security teams from detecting and managing real threats.

• **Building on generic models:** Contrary to popular belief, most AI systems only provide a small extension beyond previous rule- and signature-based approaches. Most AI deployments distribute generic models that don't understand the networks they are deployed to, making it easy for cybercriminals to avoid detection.

• **The human-AI breakdown:** Most AI systems that are currently deployed serve human users seemingly random information but don't explain the reasons behind them, leading to a breakdown in trust. When AI systems cannot support their decisions with explanations that security teams can understand, the teams must take on extra work to comprehend why the AI systems make certain decisions.

Coin Mining and Botnet Malware

Bitcoin was one of the biggest trends as blockchain took off. With it, coin mining emerged in two forms: malware on comprised assets and in-browser mining that persists only through the browsing session. As miners worked to uncover Bitcoins, companies saw a 1,500% increase in coin mining malware, according to eSentire research. The research also found that in 2018, the use of botnets increased 500% over 2017, leading to a 250% increase in overall intrusion attempts.

Coin mining malware mines cryptocurrency (typically Monero) directly on infected endpoint devices, such as CoinMiner, or in web browsers, such as Coinhive, when a user visits a website that is running malicious code. Once infected, the coin mining malware silently mines cryptocurrencies while consuming a significant amount of processor cycles. The result is devices with slow, sluggish performances and reduced battery lives.

Cloud Adoption will Pose Less Risk

As mentioned above, 72% of respondents reported that they have adopted cloud-based technologies to increase business performance. Since cloud is now in its second decade, companies are adopting more mature and proven methodologies to secure the cloud. Though cloud security is still critical, the report found that the overall risk posed by cloud over the next 3 years will drop by almost 20%.

In the coming years, cloud will expand to ERP and become the foundation in which security services are built. Cloud will move beyond application-level services to offer a foundation for enterprise-wide systems. The report found that within 12 months, infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) will rival software-as-a-service (SaaS) cloud deployments at around 95% adoption.

As cloud becomes the basis of security services, it will be imperative that organizations take proactive measures to ensure that valuable assets are secure against potential threats.

Traditional MSSPs will Shift to Proactive Hunting Services

Traditional endpoint security measures are similar to mall cops: They can detect the most obvious cybercriminals and prevent them from wreaking havoc but cannot identify bad actors who can evade detection. Businesses need to update their mall-cop approach to cybersecurity to Navy Seal-like cybersecurity measures that are able to spot deceptive adversaries, swiftly neutralize the threat through automated blocking, or engage in endpoint isolation/containment to stop attacks from spreading.

For the organizations that are adopting cybersecurity technology, traditional managed software service providers (MSSPs) only provide protection on a mall-cop level and don't provide the full protections that modern cybersecurity threats require. The research found that these traditional MSSPs only have a 45% customer loyalty rate and focus on less mature security offerings. This rate will mark the shift from compliance-centric security to proactive threat-hunting services.

These proactive threat-hunting services offer organizations more peace of mind, because they know they'll be getting Navy Seal-like protection against potential threats, especially those occurring through emerging tech channels that require new approaches. As security threats become more pervasive and damaging, proactive threat-hunting services work to stop the attacks before they seriously damage an organization.

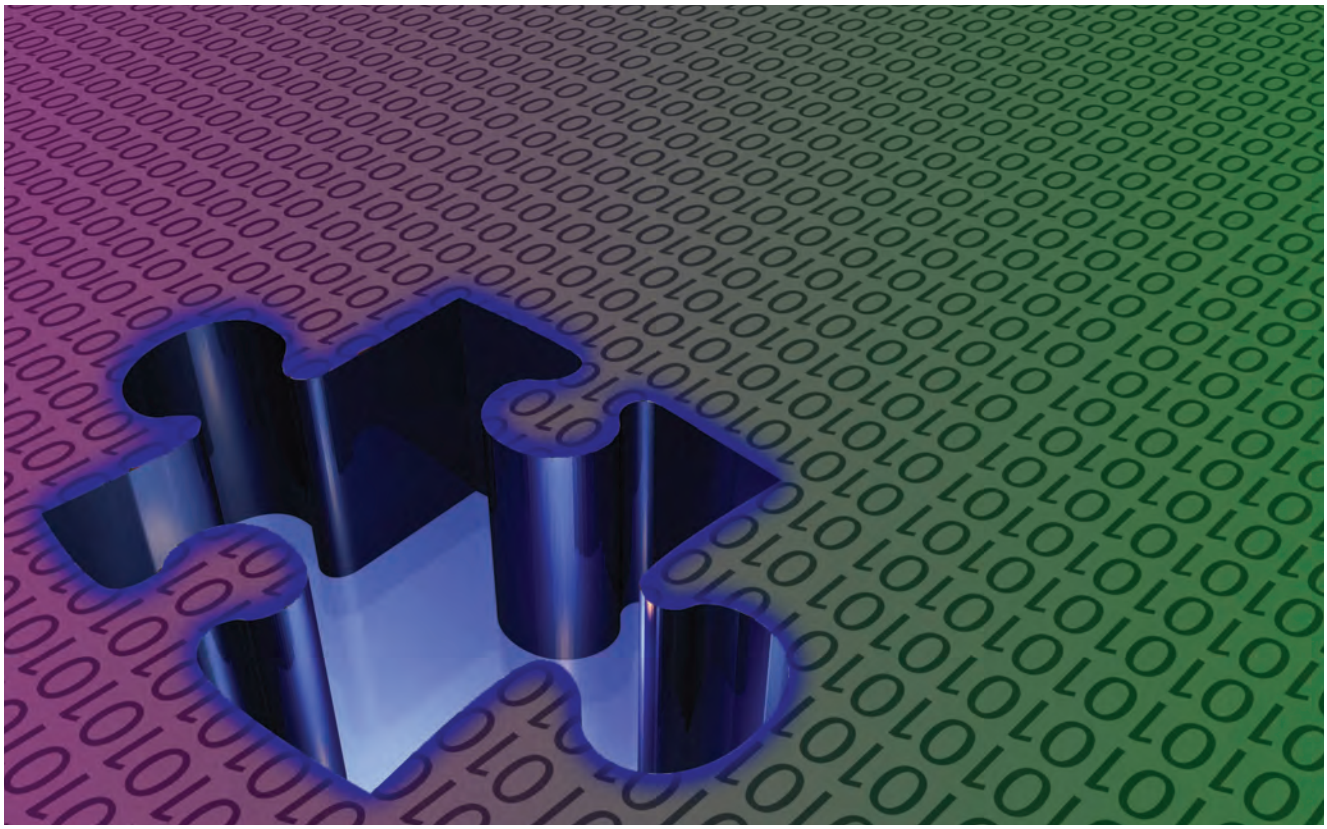
Moving Beyond a Compliance 3.0 Model

Over the years, the cybersecurity industry has been moving through device-focused (Compliance 1.0), alert-focused (Compliance 2.0), and threat-focused (Compliance 3.0) stages. It is expected that the market will transition from today's regulatory- and compliance-driven security to prevention technology. This shift can be attributed to the need to maintain business integrity and continuous operations through proactive and predictive threat management.

Currently, organizations are moving from a Compliance 1.0 model that is based on meeting the minimum regulation requirements toward Compliance 2.0: preserving a brand, protecting operations, and avoiding financial losses are the drivers of such change. In the coming years, Compliance 3.0 will center around threat-focused measures. As companies move toward the Compliance 3.0 stage, brand and reputation will determine how their security performance is measured. When companies protect the client, they will be protecting their data and services by extension, avoiding the operational disruptions and financial losses.

Cybersecurity is a business hurdle that companies can't afford to ignore as emerging technologies become core to their ability to compete. When its entire C-suite and board are made aware of what they need to know about cybersecurity attacks, an organization can take the first step toward creating a proactive, Navy Seal-like approach to stop threats in their tracks. ■

Mark Sangster is chief security strategist at eSentire (www.esentire.com), a provider of software for managed detection and response. A member of the LegalSec Council with the International Legal Technology Association (ILTA), Sangster is a cybersecurity evangelist who has spent significant time researching and speaking about factors influencing the way that legal firms integrate cybersecurity into their day-to-day operations.



The Perils of Ignoring Employee 'Leaver' Data in Regulated Industries

By Bill Tolson

Everyone leaves an employer at some point. Better opportunities, reduction in workforce actions, termination, or management issues can all result in an employee departure. No matter the reason, everyone eventually leaves the company they work for.

In Europe, these people are referred to as "leavers," and depending on the circumstances, more colorful names. However, the way a company handles these departing employees can mean the difference between business as usual or major customer satisfaction issues, project delays, higher e-discovery costs, compliance risks, and lower productivity.

When an employee is terminated or leaves on their own, the company's HR organization (if present) usually pulls out a checklist of things to do before the employee departs. In many cases, the checklist does not address the most valuable employee asset … information.

Is Leaver Data Valuable?

At its base level, companies employ people to create, process, and utilize information. What happens to the gigabytes of data the employees create and store over their time at the company? True, much of that valuable data is stored on the employee's laptop and nowadays in their OneDrive cloud account. But how long do those laptops sit around before they are re-imaged and re-tasked and how long does an ex-employee's OneDrive account stay available?

Last year, I received a call from a panicked ex-coworker at a company that I had left a couple of years prior. The person was looking for the pricing/ROI calculator that I had developed more than a year ago. A large deal was dependent on the company producing a believable return on investment proposal using the calculator. I told the ex-coworker that it and all my content should be on my laptop and in my OneDrive account. Later that day, the same person called back and told me that the company's standard process for departing employees' laptops was to re-image the hard disk after 30 days and distribute it to incoming employees and, to reassign Office 365 licenses to new employees—causing my email and OneDrive data to be lost. The ROI

model I had spent more than a month developing was gone forever.

Why don't companies capture and archive valuable departing employee data?

If not managed as a valuable company asset, much if not all that employee data is, if not lost, extremely difficult to locate or impossible to find when needed.

*When responding to discovery, you must look for **potentially responsive** data in all possible locations, unless you can prove that data **could not exist**.*

Chaotic Data Management Makes Companies a Target

Another problem associated with ex-employee data is e-discovery.

Imagine that you are a general counsel at a 5,000-person company, and you receive an e-discovery request asking for all responsive data about a specific vendor contract between Feb. 4, 2009, and last month. Several ex-employees are named as targets of the discovery.

This is a common situation many companies face. The issue is this: When responding to discovery, you must look for potentially responsive data in all possible locations, unless you can prove that data could not exist. The legal bottom line is this: If you don't know for sure that data doesn't exist somewhere, then you must search for it, no matter the cost. Legal teams have become very adept at finding the opposing parties' weaknesses, especially around data handling, and exploiting it to force them to spend more money—in the hope that they will settle early.

Another legal situation occurs when an ex-employee sues the company for wrongful termination (a common occurrence) many years later but within the local statute of limitations. Many general counsels want to review the ex-employee's data to look for information to support their defense. In some cases, judges have ruled that laid-off employees should be treated as potential legal threats and therefore under the Federal Rules of Civil Procedure (FRCP) "anticipated litigation" rule, it is necessary to keep the data for at least the statute of limitations.

Time is Not Your Friend

An e-discovery response carries with it a time constraint. The time required to respond has caused many companies to spend huge amounts of money to bring in high-priced discovery consultants to ensure discovery is finished correctly and on time. Ex-employee data can dramatically lengthen the e-discovery process.

The Departure Process Should Include Technology

Even worthless data can be extremely valuable when you cannot find it—as with the example of my ROI spreadsheet. Most companies I have worked at were very good about having standard employee exit processes. But so far, I have never had an HR (or other) employee ask me specifically for all the locations my data could be residing.

Laptop and cell phone content are turned in and quickly re-imaged (losing all data), file shares with work files and PSTs are eventually cleaned up destroying data, and Office 365 accounts are closed disposing of all email and OneDrive data. Very quickly, all employee data (intellectual property and know-how) is lost.

All it takes to solve the problem of lost employee data is to first develop an exit process that ensures the company knows where all data is and protects it before they leave—and second, migrates all data to a central repository for long-term archiving and management. Many companies are finding that a low-cost "cool" cloud archive is the best and lowest-cost answer.

Just because an employee has departed does not mean their intellectual property also has to leave. Therefore, keep ex-employee information available for business use, litigation, and regulatory compliance well into the future.

How to Manage Inactive Mailboxes When Moving to Office 365

As companies move from Microsoft Exchange on-premise to Office 365, a potential challenge Exchange admins face is how to manage the numerous inactive mailboxes. To speed the adoption of Office 365, Microsoft currently allows their customers to designate inactive mailboxes in Office 365 at "no charge" meaning they do not require a license. However, migrating and setting up inactive mailboxes is a convoluted process that involves migrating the inactive mailbox to an active Office 365 mailbox and then designating it as inactive. As a result, the Office 365 license can be reassigned.

Utilizing an Azure-Based "Leaver" Archive

Another more sophisticated option is to migrate inactive mailboxes to Azure and manage the data with a compliant data archiving platform such as Archive2Azure. Archive2Azure leverages low-cost Azure storage tiers to store inactive mailboxes, PSTs, files, documents, and all forms of unstructured data. The data is held securely and managed with automated retention and disposition. It can be easily searched, and results can be exported for further e-discovery processing. Best of all, administrators can keep terabytes of data secure while offloading the burden from on-premise network storage. ■

Bill Tolson is VP of Archive360 (www.archive360.com) and is focused on the archiving, migration, governance, regulatory compliance, and cloud-based storage of data. Tolson has extensive experience in e-discovery and archiving/information governance from both a marketing and customer perspective.

The Cost of Noncompliance:

User Consent Is a Very Expensive Issue

By Rasmus Skjoldan

"Hey Google, what's the cost of noncompliance?" Failing to comply can cost you $56.8 million—the dollar figure Google owes for breaking the EU's General Data Protection Regulation (GDPR). While this multi-million dollar mistake delivers a hit to the tech giant's reputation and checkbook, it has far-reaching implications for any organization with an online presence.

Google's largest-so-far GDPR fine was based on severe infringements against the essential framework of the regulation: Google failed to provide a transparent, accessible way for users to consent to its data policies. To give consent—and opt out of previously opted-into advertising personalization—users had to navigate Google's platform and complete several steps. Users were also unaware that by opting into one service (YouTube or Google Maps) they were opting into Google's entire service suite.

The issue and fine are so inflated because Google's economic model is based partly on its data-driven advertising personalization and the revenue those ads create. Yet, the nearly $60-million fine still represents less than half of the profits Google earns from user data each year.

GDPR Beyond Borders

Google probably won't be the only enterprise humbled by a hefty bill from the EU. Every enterprise that touches the data of EU citizens is required to comply with GDPR—that's 52% of U.S. companies and 500 of the world's largest corporations. If the purpose

of Google's fine was to send a message to other corporations collecting mass amounts of user data, the message rang loud and clear.

Severe noncompliance penalties and a growing number of consumer watchdog groups necessitate a major change in how enterprises (inside and outside the EU) protect and manage user data. Consent forms can no longer be cleverly hidden on websites and every data use case must be clearly highlighted to users, requiring clear consent before personal data is collected.

Once the use of data is explicitly spelled out, only a small segment of consumers will be willing to volunteer their personal data to the corporation. This could result in a shortage of data for targeted ads, leading to decreased effectiveness and inflated prices. If enterprises wish to continue tailoring their marketing initiatives to the user, then they need a platform that inspires users to trust them with their personal information.

*Severe **noncompliance penalties** and a growing number of consumer watchdog groups necessitate a **major change** in how enterprises (inside and outside the EU) protect and manage user data.*

Remaining Compliant With a Modern CMS

To stay compliant and keep users confident, enterprises need a reliable content management system (CMS). A modern CMS takes the guesswork out of GDPR compliance and assures users that they are in control of their data—even after they consent to its collection.

- **Managing Consent**—A CMS ensures that users have a clear path to either give or withhold consent, including website cookies. This happens during the form-building process with a set of privacy-aware templates used to collect personal data and obtain consent. In this way, consent is obtained directly on the form where the user is already filling out information. When the user submits the form they receive a double-opt confirmation in email. This makes sure that consent is genuine.

- **Storing Personal Data**—Enterprises are only allowed to capture personal user information if the data is stored and cataloged according to the GDPR standards. The CMS should assess the data against GDPR rules and store it accordingly. Data storage rules extend to mobile apps, requiring data encryptions that protect the data no matter where it is accessed. Users also have the right to be forgotten. The CMS should provide a way for users to delete their data from storage with a request form followed by a confirmation email.

- **Accessing Personal Data**—A large part of the GDPR involves user access to data. If users request their data, organizations must present the data in a timely manner. A CMS with viewable and accessible data repositories keep enterprises compliant. The CMS can export a file of all the personal data collected, from a user. This file includes the data collected, the reasons why it was collected, and a list of any third parties with which the data may have been shared.

For organizations around the world, GDPR has changed the nature of personal data collection. Across industries, enterprises are updating their CMSs to keep pace with strict regulations. By streamlining the way in which user data is obtained, stored, and accessed, leading enterprises can be sure they are compliant and avoid learning the lesson that Google did. ■

Rasmus Skjoldan is chief marketing officer for Magnolia CMS (www.magnolia-cms.com), an EU-based open source content management system.

Protecting Against Cryptomining Malware in 2019:

A Layered Approach to Device Management and Security

By Tim Williams

No single tool can ensure perfect security. That's why layering multiple tools and approaches is considered a best practice to reduce vulnerability to attacks. It has become more apparent in recent years that management tools form a vital security layer. Think of it this way: A window lock is a security tool. Closing the windows is management. Neither is enough by itself.

Trending Threats

While ransomware had been the most common and widespread cybersecurity threat for much of 2017, 2018 saw the rise of malicious cryptocurrency mining. Hackers use a simple strategy: infect a PC, smartphone, or another device with malware and discreetly hijack the processing power of the target's devices to mine for untraceable cryptocurrencies such as Bitcoin or Monero.

McAfee Labs reported in June 2018 that coin-mining malware had grown 629% compared to Q4 2017. It's an incredibly lucrative (and largely anonymous) scheme that can sap your devices' performance, cause hardware damage, and net huge amounts of cryptocurrency for hackers. Their exploits have expanded to steal credentials from popular cryptocurrency platforms via spammed email campaigns, and even include "drive-by attacks" where the cryptojacking takes place inside the web browser from an open API. Between the diversity of their approaches, the untraceable aspects of most cryptocurrencies, and the proliferation of malware and related exploit kits, cryptojacking is expected to continue its growth in popularity for cybercriminals and become an even bigger problem in 2019.

Symptoms of Cryptojacking

It's important to know what to look for when diagnosing a potential malware-driven issue. If your device has been cryptojacked, you may hear loud whirring sounds from your desktop or laptop. Your device may heat up and battery life for mobile devices will drain faster than usual. Performance on your device

may be impacted as well, running programs more slowly and even crashing while performing tasks that had become part of your normal routine. If it's your company server that's been hijacked, you may see issues with web performance and crashing. Over the long-term, you'll see spiking electric bills due to the increased energy draw from your device.

While cryptojacking may seem less damaging to those under attack than ransomware, you should not underestimate the impacts. System overloads due to discreet cryptomining can disrupt business and threaten infrastructure should critical systems become compromised. Secondary leaks of personal information, financial accounts, and other data breaches can be costly and put your customers at risk.

While the symptoms outlined above are not unique to cryptomining attacks, there are system performance and management criteria that can be monitored and reported to help identify new threats.

Identifying the symptoms is only the first step toward diagnosing and curing the problem. Similar to a parent with a sick child, your management tool can figuratively take the temperature of your systems and call the security doctor. An ounce of prevention is worth a pound of cure. While no single solution stops all threats, managing devices effectively adds a vital layer of defense that can help reduce security risks to corporations and individuals.

Security: A Layered Approach

When it comes to cybersecurity, many organizations are investing solely in more security tools to manage risk. Unfortunately, this cannot create a perfectly secure organization. Security is far less effective without strong management protocols; you have to make sure the tools in place are being used effectively in order to protect against cyberthreats. By reinforcing foundational behaviors and keeping effective processes in place, you're making sure that your team closes the window before they lock up. This can be done with the help of innovative and automated functions within a robust endpoint management solution.

Patch Management

At least 60% of organizational data breaches are due to unpatched vulnerabilities in both applications and operating systems. If you believe your users are all up-to-date on their system critical patches, think again—users frequently defer update processes to avoid potentially lengthy installation downtimes. Those gaps, fueled by end-user ignorance of the vulnerabilities, can create easy opportunities for criminals to gain access to devices and sensitive data. When you factor in the increasingly diverse device landscape filled with fragmented OS updates, the sheer size of the management task can be staggering.

IT admins need a simple and effective means to manage patch deployments from a centralized dashboard where they can track compliance and ensure these risks are being prevented. Automating deployments and compliance is a crucial aspect of layered approach to IT security management.

Even on patched systems, management tools can detect, for example, Windows services or processes that are running for the first time, which could be an indication of a zero-day attack.

Maintain Security Tools and Settings

In addition to plugging security gaps left by unpatched software, ensuring compliance of security tools is essential. Deploying critical security software is worthless if it is not maintained. Users seeking a way around VPN or firewall configurations can unintentionally damage or alter critical files and updates, putting security at risk. Well-intentioned but misguided users may utilize "shadow IT" to try and solve problems, sidestepping compliance processes and introducing more unknowns to your IT system.

Automatically repairing and replacing anti-malware, VPN clients, and other tools can reduce these issues. This automated self-healing can detect, repair, and reinstall missing and corrupted applications and associated updates that have been altered by either the end user or an outside system intruder. The protection and peace of mind afforded by this functionality is vital for protecting against cryptojacking and other attacks.

Manage Your Network

For cryptomining malware, IT servers are a prime target due to their increased processing power. Unmanaged or rogue devices can pose the greatest threat to your system and become a backdoor access point to your IT.

Making network discovery a cornerstone of your security protocol can show you what's out there, identify non-compliant systems, and help remediate issues with devices, applications, and settings. Think of this layer of defense as checking who's at the door before you open up your home and invite them in. A single console multi-platform management tool can provide you with the visibility needed to detect the threat and fix the issue before it causes a breach.

Future Security Developments

No single solution will mitigate all risks to your IT security. Layered management is designed to reduce risk at each security level by creating multiple levels an intruder would have to breach to access data and implement malware. In addition to the behaviors already discussed, investigating loud fans, slow devices, and other signs of overloaded hardware can turn up intrusive software. Training and educating your staff in recognizing and preventing these risks is essential—a robust endpoint management software will help manage the devices, but you cannot mitigate all risks without the buy-in of your end users as well. Your people are a fundamental layer of a holistic approach to layered management. Maintaining each layer of your device security and adapting those layers based on changing threats is a critical step in protecting your organization against digital intruders. ■

Tim Williams is VP, global marketing & product strategy, at FileWave (www.filewave.com). During more than 25 years in multi-platform endpoint management and endpoint security, Williams has led global sales, marketing, and product management teams at companies including Netopia, Altiris, Symantec, and HEAT Software.

The Right and Left Brain of DevOps and Security:

How to Gain a Meeting of the Minds Instead of a Battle of Wills

By Gary Southwell

Considering the importance that applications play in operating and/or driving commerce in many organizations, it is no wonder that DevOps is the crucible for these businesses' long-term health and realization of their roadmap.s In some enterprises—such as Amazon, Airbnb, Netflix, and Uber—the application set is the business. In others, there is more to the business than just the app—but the app plays a critical role to an initiative or process. The monumental significance of apps in either case has required the DevOps team to work with ingenuity, clarity, speed, and deep pragmatism in turning thoughts, ideas, and intended experiences into reality.

DevOps teams serve the needs of the business—typically a business owner or group funding the effort. They set the requirements of what it must do—focusing on capabilities, performance, time-to-deployment, analytics, and other concrete must haves. Making it easy to use and quick to deploy typically requires masking large amounts of complexity and a myriad of backend operations necessary to provide the highest levels of functionality and ease of use. These lofty goals in addition to the high impact of the work have led to the no-holds-barred, unconstrained, and inventive working style. These needs have fostered traits

in the DevOps developers akin to a kind of right-brain orientation. Software development becomes a bit of a creative art form that produces innovative approaches that are tried and iterated—discarded if they miss or evolved if they don't—through a set of releases leading to a production candidate.

This streamlined approach is elegant, yet potent. The operations side of the house provides the infrastructure on which the applications run and thus the data needed for testing and deployment. It oversees and maintains the applications, the inputs into them, and the security of the data. The operations side is more left-brained—grounded in a focus to enable the application to be deployable, scalable, and maintain stable performance for a variety of foreseen deployment condition scenarios. Both teams report to the business owner, are tied to a funded project, and ultimately aligned in their end goals to produce a working product.

Then there is security. Security is not natively oriented in the flow of the business or customer engagement. Typically, it is a separate corporate IT and/or networking function. The staff is analytical and driven by processes to minimize risk and offer protection from bad actors inside and outside the organization. Additionally, security teams focus on finding the holes that may expose data to possible theft and identify policy violations. Security is very left-brained and sometimes considered the "anti-DevOps" team because its goals are not aligned with those of the business owners funding a particular DevOps project.

To further elaborate on the conflicts, while DevOps embraces creativity, security embraces repeatable, consistent processes. DevOps is driven by speed and progressive accomplishment; security is driven by reduction in risk. Even on the operational side, DevOps wants fast, responsive apps with ease of access, while security favors locking down data and applications, applying layers of mechanisms that slow deployment and possibly performance in order to protect the application and the data it accesses. Security is the team most likely to address compliance issues and requirements, working with auditors to assure compliance with rules and regulations. Compliance needs to "think global and work local" by considering international markets with regional requirements. Generally, this has as much or more to do with data accessed or generated than the actual coded application. These people read and shudder at the Equifax case study: How their lack of proper InfoSec had allowed a flawed application to access a flawed internal set of processes which led to the complete compromise of all their critical data. The fall-out has been severe, with many losing their jobs, including the CEO and many of the senior staff from its security team. Thus, security is adopting the following mantra: I am the guardian of the keys to our kingdom—or there we go.

*While **DevOps embraces** creativity, security embraces repeatable, consistent processes. Similar to the human brain, the two hemispheres—the right side within DevOps and the ultra-left with **security and compliance**—are separated by a groove or chasm.*

Similar to the human brain, the two hemispheres—the right side within DevOps and the ultra-left with security and compliance—are separated by a groove or chasm. Humans have the longitudinal fissure, which is really just space that demarks the two sides. Given their important charters, security and DevOps groups are relatively autonomous and often have little daily interaction with each other. Reporting structures are vastly different, and both groups are given carte blanche to pursue their missions. It is of little wonder why the two sides are at odds.

The separateness and divisiveness, however, are problematic and not sustainable. It is inefficient and cumbersome to sequentially develop an app and hand it over to security for review. Even worse is the practice of developing and deploying an app and then having it flagged for problems and shut down—or, worse still—missing problems entirely and allowing an under-secured application into production (POS systems, industrial IoT, connected cars, to name a few well-publicized failures).

It is too time-consuming to tack a security review to the end of a development program. The security team has to play catch-up with unfamiliar code and architectural plans. Changes imposed by security may be larger at the end of the process, imposing a great impact on the access, functionality, and performance. It could be a massive issue, requiring long, expensive, complex operations and potentially presenting a risk to the life of the project.

Waiting until the end of the development process to address security issues makes no sense—the compromises will be larger and addressing them may involve much more deliberation and work between teams. Aspirations of great utility and ease-of-use may suffer far more when the security review is at the end of the process. Leaving security to the end results in longer release delays, greater expense and resource involvement, and bigger compromises to both sides.

The forward-thinking enterprise realizes that having two separate hemispheres is no longer viable. The right and left sides must work together from the very beginning—just the way we have the application development teams working daily with operations. Security needs to be brought in to collaborate on the app design or at least to apply security controls earlier in the deployment phase without invoking the development team is the right path forward.

Achieving a more integrated process that brings security, application development, and operations together from the beginning, to form SecDevOps, involves some substantial changes … or does it?

One of the first necessary changes is charter and accountability. Security and DevOps must both understand and participate in goal setting for the business. The business owners must acknowledge and include risk mitigation as a key business goal. This can start with an analysis as to whether the desired application may create a significant risk to the organization—usually

determined by whether the application is touching or is generating critical production data. If yes, there is great risk, and, if not, then it is minimal.

The decision about what level of risk the enterprise is willing to take on in order to accommodate important business initiatives should be set at the board of directors level. While this may not seem to be a typical board of directors or senior corporate management standing agenda item, it is becoming one. Security studies from Kaspersky Labs, as well as the Ponemon Institute have found that significant data breaches have not only cost organizations millions of dollars but, in about 25% of the time, prompted the dismissal of senior corporate executives. The new reality is that regulatory compliance changes are driving board decisions, as well as cyber-risk assessment especially as the realization grows that breaches do substantial long-term injury to businesses.

Once it is acknowledged that risk mitigation is a driving business requirement, it is easy to change reporting structure. Proximity also has a positive effect on communication, cooperation, and understanding. Giving security a vested interest in the success of a secure digital initiative and the business it represents ensures better integration and more attractive results.

Another important change is to move the process from being sequential to one that is more parallel. Get the security experts involved with incorporating security values and features early in the application development process. Security experts can assess third-party libraries and code for vulnerabilities—ensuring that the latest versions and patches are applied even before they are added to the next iteration of code base. Incorporating security early in the process eliminates the substantial standstill that results when security reviews an app after its creation and has to review and analyze unfamiliar code and designs. Catch-up can be eradicated with security participating in the development process from the start. Decisions about trade-offs between risk and functionality can be made fluidly along the way. Most DevOps works around a model of continuous development and integration to enable better apps with less delay. Security should also be seamlessly worked into that model to prevent a right brain-left brain clash with unfortunate results.

While security needs to work alongside development, within the continuous development and integration context, having vetted code libraries and registries proves productive in providing security functions that can be incorporated by developers. Many DevOps teams favor utilizing available code to avoid wheel reinvention in order to achieve challenging sprint deadlines. Incorporating security routines fits nicely with this model and likely results in better production software. Often, right-brain software developers lack left-brain security expertise, particularly with cryptography and authentication processes.

Unfortunately, such off-the-shelf security code generally does not exist. It's time to create repositories to share such code. Capabilities such as these still have to be integrated within the applications and can have a negative impact on performance if underlying compute is not available to handle CPU-intensive tasks typically required by the proper application of cryptography on a per-application or per-access identity basis. The work requires decisions around the necessary security capabilities required to minimize risk. For example, if stolen drives are the only risk, a single crypto-operation can be run across all operations that need to store data on a disk. However, most organizations realize that attackers landing on a device would likely get access to all such data if any users' credentials were compromised. Best-practice approaches known as security-in-depth—would limit the amount of data at risk by providing unique-keyed encryption on a per-application basis, or limit further if deployed on a per user or even on a per-transaction basis. Ideally, developers would have to make no such decisions but merely connect in the proper security code that would allow the InfoSec team to set the appropriate level of protection within the application at the time of deployment. Done once, the process can be automated so that the application can be properly initialized and have its security settings configured on an automated basis.

It's time for the right and left hemispheres of the brain to come together. The demands on DevOps and InfoSec continue to grow and the risks also tend to escalate as the applications become more important to the organization. Putting these teams together is a no-brainer. Yet it's critical we give them the proper mandate and tool sets that allow them to be effective in achieving all business requirements, including security, while also meeting important business deadlines on budget. ■

With over 25 years of strategic business and security product planning, **Gary Southwell** brings a wealth of data privacy and compliance knowledge to his role as general manager, Security Products, at CSPi (www.cspi.com), which is committed to helping customers meet some of computing's most demanding performance, availability, and security challenges.

Meet the Data Privacy Challenge: Creating a Culture of Responsibility

An organizational shift is necessary to adapt to constantly changing regulatory requirements and satisfy new ethical concerns

By Amandeep Khurana

Google's stiff fine for non-compliance with the EU's General Data Protection Regulation (GDPR) has demonstrated the potential impact on a company's bottom line in a way that has made GDPR a topic of discussion in many corporate boardrooms. Yet, a recent study by IT Governance revealed that only 29% of European-based organizations are GDPR-compliant. It has been speculated that the situation is even worse in the U.S., where the passage of the California Consumer Privacy Act (CCPA), along with proposed new federal privacy standards, means that organizations will continue to face a rapidly evolving and increasingly complex regulatory compliance landscape with ever higher stakes.

What's needed is a dynamic governance environment that allows an organization to constantly adapt to both evolving regulations and the rapidly changing data infrastructure. However, the only way to achieve this environment is to create a foundational "culture of responsibility."

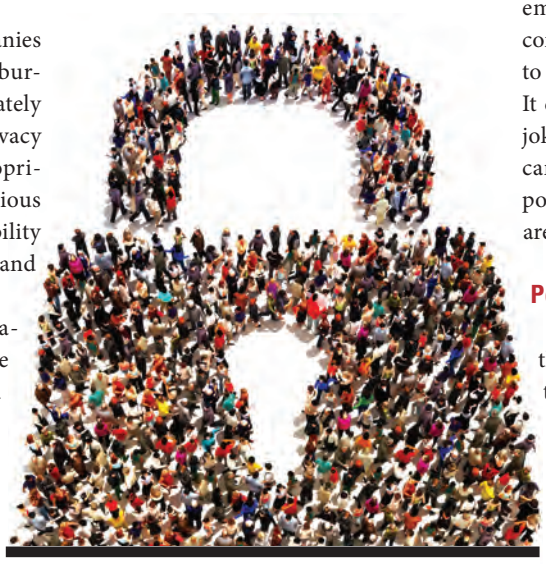
Why It Matters

While the actual and potential fines related to GDPR and the CCPA are generating the headlines, there is more to the data privacy challenge than just meeting specific regulatory requirements. The amount of personal

information that companies collect continues to skyrocket with data lakes growing to petabytes in scale. Further, thanks to abuses of personal information at Facebook and other companies, consumers are taking an interest in how the companies they deal with treat their information. This means companies now need to consider the impact on reputation and consumer confidence of their data governance strategies and effectiveness.

However, even well-meaning companies are struggling to govern their ever-burgeoning data stores. They can't accurately identify what data falls under which privacy regulations. They can't ensure appropriate usage consistently across their various data platforms. And, most lack the ability to audit their internal data processes and demonstrate compliance to regulators.

On a more tactical level, a fundamental friction exists between those charged with protecting data and those who need to use the data for business purposes. An expanding range of business users sees data as their resource and want fast, self-service access to it, and they often see data stewardship as an obstacle to ease-of-access. Meanwhile, data stewards and platform teams see their primary responsibility as securing the data and supporting regulatory compliance. A successful governance strategy must bridge this divide.



*A successful **data governance strategy** must bridge the divide between business users who want self-service access and data stewards who see securing data as a **primary responsibility**.*

A Culture of Responsibility

Such a governance strategy requires a fundamental shift in how organizations think about data governance and privacy. Consider the different attitudes toward privacy expressed by Google/Facebook versus Apple. At companies such as Google and Facebook, collected personal information is a product, and the revenue to be generated by that product will, at a minimum, inevitably lead employees to blur the line between uses that have been clearly authorized through customer consent and those that haven't. Meanwhile Apple's Tim Cook, in a recent speech at a privacy conference in Brussels, acknowledged that protecting personal information is critical for our society. After praising the EU's implementation of GDPR, he said, "It is time for the rest of the world ... to follow your lead. We at Apple are in full support of a comprehensive federal privacy law in the United States." He also addressed the complaint that such regulation is a barrier to innovation, saying, "This notion isn't just wrong, it's destructive."

Accepting that privacy regulations are not a barrier to innovation is the seed that needs to grow into a culture of responsibility.

As with the shaping of all corporate cultures, creating a culture of responsibility requires a vision actualized by people, processes, and technology. Leaving out any one of these elements will doom the initiative to failure.

Vision

The vision underlying the culture of responsibility is that managing data in a way that protects personally identifiable information and enables regulatory compliance is a corporate asset, not an operational burden. Companies that successfully govern their data benefit in many ways, including better business decisions, greater agility, increased consumer confidence, and reduced costs associated with, for example, regulatory fines, legal discovery, data storage, and low employee productivity.

Most importantly, this vision must be embraced as something that makes the company better and stronger, that is critical to reaching the company's strategic goals. It can't be seen as a burden, an obstacle, a joke, or an afterthought. The only way this can occur is if top executives, including, potentially, a chief privacy officer (CPO), are frequently seen making this embrace.

People

Once company executives describe their vision for a new strategic initiative, they often assume the people working for them will automatically put in place the mechanisms to make that vision a reality. However, the "people problem" may well be the most difficult challenge to overcome when attempting to change the corporate culture. No matter what technology and processes are instituted, employees will have the ability to develop work-arounds, create new shadow IT, lie, cheat, or even inadvertently find a way around a proper procedure.

Preventing—or at least minimizing—this starts with executive accountability. It simply isn't enough for executives to "support" a policy. They must take an active role in ensuring the implementation of that policy and hold themselves—and their peers—accountable when the policy isn't implemented correctly or in a timely way.

When it comes to the culture of responsibility, it's also essential for executives to understand that we are no longer talking simply about checking off boxes on a regulatory compliance cheat sheet. Privacy is an ethical responsibility. All employees should understand that they are custodians of customer data, and just as they would want their private information protected at

other companies, it is their job (not somebody else's) to protect their customers' data. It must also be made clear that when this ethical responsibility comes up against revenue potential, ethics must win. Representatives of public companies often discuss their fiduciary responsibility to maximize profits for their shareholders, but it is time they recognize that today, as demonstrated by Google and Facebook, abusing private information will ultimately have a negative impact on profits.

Operationalizing this attitude may not be easy in many organizations. For many companies, it will require the addition of a CPO, who will have the power and focus to create the culture of privacy. It will also require ongoing training and regular reinforcement. Creating a document or presentation that announces the vision and lists the commitments simply isn't enough. The culture of responsibility must be reinforced at every level of the organization.

Processes

To create a culture of responsibility, privacy and auditability must be designed into every step of every process lifecycle. And existing processes may need to be redesigned to incorporate privacy at every step. Whether it's customer onboarding, product or service design, or customer upsell programs, process designers need to take responsibility for what is happening with the data. Just asking people to be better isn't going to suffice. The systems and processes in the organization need to enable and incentivize the right behavior. For example, designing distributed stewardship that's scalable and agile will enable the broader organization to work toward the agreed upon goals. Meanwhile, centralizing all stewardship responsibilities will quickly create a choke point and incentivize people to find workarounds.

Technology

In the era of big data, with data increasingly stored in multiple clouds and on IoT edge devices, securing and governing data in a scalable and agile way is technically more difficult than ever. As of yet, there is no standard way that security and governance capabilities fit into the big data journey, even as a growing array of data users—including data engineers, data scientists, and business analysts—are demanding fast, self-service access to the data in massive data lakes using a variety of analytics and machine learning tools.

The result has been the creation of fragmented solutions that make copies of data and otherwise increase the risk of inconsistent compliance. To support a culture of responsibility, organizations must adopt a governance solution that adheres to the following core tenets. It must be data-centric and independent of the applications being used to access the data. It must provide the required level of access control for both structured and unstructured data. And it must automate enforcement. Such a solution should also take a holistic approach to visibility into the data, providing fast, simple insight into both past access patterns, the data any particular person can access, and who has access to a particular data asset. Finally, an effective solution must future-proof the organization to handle the frequent and significant regulatory and technology changes it will face over the coming years.

Failure Will Be Costly

The ability to comply consistently with evolving privacy regulations is now a core competency for every organization. Those that approach developing this competence from an ethical perspective, creating a culture of responsibility that empowers every employee to support the compliance goal, will ultimately achieve that goal faster and at lower cost. Most important, they will future-proof their organizations against the inevitable regulatory changes while enabling agility and innovation without the fear of compromising the ethical necessity to protect their customers' and employees' private information. ■

Amandeep Khurana is CEO and co-founder of Okera (www.okera.com), which provides the Okera Active Data Access Platform to manage data access across a multi-cloud, multi-data store, and multi-tool world—reducing friction between agility and governance. Prior to Okera, he served as principal architect at Cloudera where he witnessed first-hand the challenges companies faced in adopting big data technologies, especially in the cloud. He founded Okera to empower all users with easy data access through a unified, secured, and governed platform across heterogeneous sources.

Since 1978, IRI has delivered robust manipulation software like CoSort for data architects whose sources grow faster than their budgets.

With PCI DSS, HIPAA, the GDPR, and more data privacy laws coming online, it's also DBAs and data security governance stakeholders who now want IRI's proven, affordable solutions for:

- PII discovery and classification
- Multi-source, multi-method data masking
- HIPAA/FERPA-compliant re-ID risk scoring
- Safe, referentially correct test data
- Fast, no-impact DB firewall technology

You'll find these capabilities in award-winning IRI Data Protector suite software: www.iri.com/products/iri-data-protector

+1.321.777.8889
info@iri.com
Proven, Affordable Data-Centric Security

IRI, The CoSort Company
www.iri.com/products/iri-data-protector