PEERLYST PRESENTS

Essentials of Cybersecurity

InfoSec experts share their tips on getting the basics right

PEERLYST PRESENTS

Essentials of Cybersecurity

InfoSec experts share their tips on getting the basics right

Note: We’re sharing this e-book as part of Peerlyst’s mission to enable free and authentic information flow in the space of information security. Our authors are members of the Peerlyst community of InfoSec professionals and contributed this content voluntarily.

Peerlyst is where security pros like you go to learn, share knowledge, and build reputations. Join us here and get daily content like this, and much more, from thousands of security users.

Special thanks to our authors, whose insight and generosity embody the spirit of Peerlyst.

Thanks also to our editor, Maria Behan.

Disclaimer of Liability. This crowdsourced publication represents the collective efforts of the authors behind each chapter. Those authors and the publisher have made reasonable efforts to ensure the accuracy of the content of the book, but bear in mind that much of the material here is based on personal experience, anecdotal evidence, and information gathered from a variety of sources. The content contained in this book is no substitute for seeking advice from an information security professional familiar with the facts relevant to your career or organization. The publisher and authors hope this book proves helpful to information security professionals, and they disclaim any express or implied warranties.

Peerlyst, Inc.
715 Bryant St.
San Francisco, CA, 94107

Table of Contents

Introduction

By Limor Elbaz

Information security is a symphony of knowledge, actions, behavior, and tools—all orchestrated by the security team.

Security management is more than just choosing and using products. It's about building a team and creating an enterprise-wide culture of security. It requires allocating resources and managing a budget. It's also about managing your assets: your team, the company's employees, and your tools and products.

Security means understanding the different types of threats you're dealing with, and coming up with an appropriate strategy to protect your company. It's about gathering, analyzing, and protecting information. It entails managing secrets, within your team as well as your enterprise. Security management involves measuring your effectiveness, and using specific metrics to lower your company's risk. It requires understanding all the different aspects of security in a corporation—including network, endpoints, and data.

This book, *Essentials of Cybersecurity*, touches on these points and more. Our goal is to give readers some insight into the world of information security, and perhaps advance them on the path of becoming security experts themselves.

This is Peerlyst's second e-book. Like the first, *The Beginner's Guide to Information Security*, the content you'll find here was crowdsourced from members of the Peerlyst online community of InfoSec professionals. I'd like to take this opportunity to thank the ten contributors who volunteered their time and expertise for this effort. And to invite you, the reader, to join our community to learn more, connect with others, and deepen your enthusiasm for cybersecurity.

***Limor Elbaz** is the founder and CEO of Peerlyst, Inc. To hear more from Limor, follow her on Twitter @LimorElbaz, or check out her page on Peerlyst.*

Chapter One

Starting at the Beginning: Why You Should Have a Security Program

By David Froud

For those who have been in security for some time, it may be difficult to understand why implementing a security program is such an uphill struggle. After all, the administrators of a security program have an almost unparalleled understanding of the entire enterprise. From infrastructure, to process, to data, to people, security touches everything.

Regardless of what the business's goals are, it is every department's responsibility to enable those goals. But security teams are without a doubt, the ultimate goal-enablers. In my view, that is all information security is there to do: enable. Not to tell others *what* to do, just *how* to do it appropriately. Not to say no, but to provide *secure* alternatives. And finally, not to be only a cost to the business, but to represent a *true* ROI.

Why then is security so often treated as an afterthought? The reasons behind that mostly negative perception are as diverse as they are myriad, and hopefully this e-book will in some way set things straight.

Unfortunately, the security industry itself is not helping matters. The pressure to turn a profit in a highly competitive industry that already has an image problem is daunting. So instead of turning to the basics for direction, vendors and consultants alike are turning instead to buzz phrases, acronyms, and the latest shiny thing.

But when you look through all the hype, you always come back to same three things: confidentiality, integrity, and availability (CIA).

Every security program, regardless of the organization's industry sector, region, or size, must achieve an appropriate balance of these three fundamentals. To put them simply:

- ***Confidentiality*****:** If everyone else has your information, you're probably not innovating; you're doing what everyone else is doing. Maybe you're doing it slightly *better*, but you aren't going to stay in the lead for long.
- ***Integrity*****:** Not much point in making decisions if you're making them for the wrong reasons, in the wrong place, at the wrong time, or badly. If your information is not accurate and relevant, it's just data.
- ***Availability*****:** You can have all the information in the world, but if you can't get to it WHEN you need to get to it, it’s of no use.

Information security departments are the guardians of the CIA triad, and their processes are the very model of manageability, accountability, and continuous improvement.

But What IS a Security Program?

In order to put the *need* for a security program into appropriate context, we must first define what a security program actually is. If you ask 100 cybersecurity professionals what a program looks like, and you’ll get 110 different answers. For the purposes of this chapter however, we accept that these are the basic building blocks:

- ***Senior Leadership Support.*** By far the most overlooked—or entirely ignored—aspect of a security program. If the CEO/board of directors doesn’t care about security, no one else will. And if that’s the case, why even bother?
  With senior leadership buy-in, and perhaps even direct involvement, the security program takes its rightful place in the corporate culture, which is the only place it can do any good.
- ***Culture.*** While there is no “corporate culture” without senior leadership buy-in, there can be no security without buy-in from *every* employee. Regardless of an individual’s role, EVERONE must understand, and *accept*, their responsibility for the security of the organization’s data assets.

When every employee cares about security, social engineering, and malware infections, those and other ignorance-based threats are dramatically reduced.

- ***Governance Committee.*** Often the most difficult aspect of a security program to put in place, but one of the most critical. Governance is the beating heart of a security program, and is the best way of enabling the business side and the IT to have meaningful conversations. Every department should have its say, and governance is the forum for that expression.
- ***Policies, Procedures, and Standards.*** The oft-slighted "paperwork" aspect of a security program is one of the foundations of security. Policies are the do's and don't's that define the culture of an organization; procedures are the physical manifestation of "corporate knowledge;" and standards are the "known-good baseline" from which every business process is built. Get these wrong, and there can be no effective security.
- ***Risk Management.*** The primary function of risk management is to ensure that all security controls meet the organization's risk tolerance. Risk assessment, business-impact analysis, risk treatment, and the risk register all sit within this sphere. When properly managed by the governance committee, senior leadership will have the right information to make decisions based on the organization's goals.
- ***Security Controls.*** Security controls involve not just technology, but also people and processes. Any control that is not appropriate is either too much, or too little, security. For a control to be "appropriate," it must meet ALL of the following criteria:
    - It must fill the relevant gap(s), as defined by the risk assessment process
    - It must be future-proofed (as much as possible/feasible)
    - It has to be implemented correctly
    - It has to be managed correctly
    - It has to be continually optimized
    - It must be measurable and with reported metrics
    - It must be value for money
    - The purchase of new technology is always the *last* resort, as business challenges can never be fixed by technology alone.

- ***Vulnerability Management/Change Control*.** These metrics don’t get lumped together very often, but from a program perspective, they have similar results, because they don’t make things easy for the attacker by 1) ignoring the evolving external threat landscape, and 2) introducing potential internal vulnerabilities without due diligence.
- ***Testing Program.*** Every security program framework includes a section on testing (the old ISO 27001: Plan > Do > Check > Act, for example). And for very good reason: Unless you KNOW whether or not your controls are working, you have no idea what additional risks you are facing. Few organizations can afford an internal testing team, and bringing in outsourced expertise has several ancillary benefits.
- ***Management Reporting.*** As Peter Drucker is attributed as saying, “If you can't measure it, you can't improve it.” From a security program perspective, if you can’t measure the effectiveness of a control, you have no way of knowing if it meets the organization’s needs. Once again, this is about appropriate controls, as too *much* security will get in the way of the business’s function.
- ***Security Awareness and Training.*** The cheapest, and by far the best way to put both a security culture and people-based security controls in place. While technology is absolutely necessary given the sheer quantity of data, it’s the people aspect of security that makes the difference. A well-educated and constantly informed employee can make the difference between a security event and a business-crippling disaster.

The Sticks and the Carrots

In almost every security budget request ever presented to a finance committee, the motivators are almost entirely negative. Those motivators will include at least one, if not all three, of the following:

- ***Direct Financial or Competitive Loss.*** The theft of financial account data, or of research and development/intellectual property, has a direct effect on the bottom line. Not every organization will recover from the loss of significant £/€/$, or the blueprints for their latest widget.

- ***Regulatory or Legislative Penalties.*** Where the loss of data has more "indirect" penalties, the cost can be just as severe as direct loss, if not more so. For example, in Europe, Visa can fine up to €18 per primary account number lost in a breach. And the upcoming General Data Protection Regulation (GDPR) allows for fines of up to 2 percent of global revenue up to a max of €10M for loss of personal data. Per event!
- ***Reputation Damage.*** Both of the above factors can have impact on an organization's reputation, but for some this goes much further. A company that relies on the integrity of its data to deliver a service will have a very hard time recovering from a significant breach event. Or a company that boasts about uptime will be embarrassed should an event take its systems offline.

While these are valid and persuasive arguments, they all fail to hit the mark in environments with traditionally high risk tolerance (large retail for example, given its razor-thin profit margins). Unless the senior leadership has already been through a breach scenario, these arguments can fall on deaf ears. Until, of course, it happens to them.

Instead, a well-run and appropriate security program actually has a significant ROI on the business as a whole. While a good security program won't necessarily allow an organization to make more widgets, its other benefits can have just as great a positive impact. No discourse on why a security program is necessary is complete without touching on the numerous advantages.

Competitive Advantage. In the Information Age, a large percentage of businesses are almost entirely based on the manipulation and use of some form of data. Data in context is information, information in context is knowledge, and knowledge applied correctly is innovation, and so on. It follows therefore that the organizations that have the greatest ability to guarantee the confidentiality, integrity, and availability of its data assets will have significant advantages in the market.

Business Transformation. Similar to, but different enough from the competitive advantage point above to warrant its own section. Again, seeing as data is central to all things, the ability of an organization to order, compile, and retrieve accurate data faster gives it the ability to adjust processes in the face of customer needs or competitive threat. If you don't know what you have, or, in detail, how you do what you do WITH what you have, you cannot make change fast enough. Competitive advantages in the Information Age last weeks/months, you simply don't have years to catch up.

Governance Model. As stated above, governance is the forum within which the business side and the IT side have meaningful conversations about business goals. But other than accounting, few departments have likely heard of, let alone implemented, a form of governance. Security *requires* governance to be truly effective, but every other department can significantly benefit from being part of these conversations. Knowledge is power—and governance is where you get the knowledge.

Financial Control**.** All finance these days is just data in context, and while security will never be able to provide that context, access TO, and the integrity OF the data can provide a much-welcome check and balance for the control of an organization's financial data assets. Regulations like Sarbanes-Oxley (SOX) have security as part of their requirements, but go nowhere near far enough to provide much benefit. A security program done well would cover this and a whole lot more.

Cheaper IT Infrastructure and Maintenance. This may seem strange, even counterintuitive, but you only get real security when all the processes are simple, and you can only achieve simple if everything you have is a known-good, or baseline. These baselines are hard to achieve, and can be expensive in the short-term, but the long-term costs are significantly lower than trying to either constantly work with too much (technology, data, people, etc.), or to fix what's broken because you couldn't detect a problem in time to prevent it from becoming a disaster.

Automation of Internal Audit and Compliance Validation**.** We talked about management reporting above, which suggests that you must have a baseline, or norm, from which to report *against*. Policies and standards *are* that baseline, and the security controls are the manifestation of it. Both management reporting, and by extension, internal audit, are therefore the measurement of the current state against what it should be. So is regulatory compliance. It follows therefore that any automated security control (SIEM, for example) could be used to run comparisons against known-good baselines.

Marketing Kudos. In a perfect world, security would be in place because it's the right thing to do. In reality, getting senior leadership attention requires a business driver. For example, being granted a large contract if, and *only* if, an organization is Payment Card Industry Data Security Standard (PCI DSS) compliant is very common. In the EU, ISO 27001 certification will likely be more important in light of upcoming regulatory obligations. While obtaining security budget in *reaction* to a regulation is very far from ideal, as long as the money is used to implement appropriate controls, the benefits are achieved.

In the end, the effectiveness of a security program is directly proportional to the importance bestowed upon it by senior leadership. It is up to the security department to develop the right combination of carrots and sticks.

David Froud *has over 17 years experience in areas of cybersecurity, including regulatory compliance, secure architecture design, governance framework design, data privacy and protection, and sustainable innovation. As project lead for several Fortune/FTSE "Enterprise Class" clients, David has performed hundreds of on-site security and compliance assessments for merchants and service providers globally. He's currently focused on helping organizations unify their security programs with upcoming EU regulatory compliance regimes (GDPR & PSD2). To hear more from David, check out his blog, Froud on Fraud, as well as his profiles on LinkedIn and Peerlyst.*

Chapter Two

Understanding the Underlying Theories of Cybersecurity

By Dean Webb

Soldiers, Cops, and Spies

It’s popular to use military metaphors to explain cybersecurity. Firewalls, intrusion prevention systems (IPS), proxy servers, and antivirus programs are the perimeter defenses. There are attackers and defenders. There’s an arms race. Older forms of cyberwarfare were trench warfare, now it’s more like the blitzkrieg.

Yet these are highly misleading metaphors. Yes, they are dramatic and can make executives feel like generals, commanding vast armies of network devices and pointing a commanding finger towards destiny. But that simply isn’t the case. Executives aren’t generals and security people aren’t officers and PCs certainly aren’t soldiers. And the enemies might exist outside, but thinking about military metaphors can blind one to the enemies operating on the inside.

The thought of an employee being a traitor is highly uncomfortable. As soon as one person at the workplace can’t be trusted, one begins to wonder, who else shouldn’t be trusted? How does a security staff keep from descending into a fevered mob of paranoids, everyone’s back to the wall and eyes wide open? It may be more comfortable to mentally cast one’s self as the front-line commander and never ask awkward questions about what’s going on behind the lines.

Security is not about comfort, though.

To be sure, the military metaphor is not entirely without merit. There are millions of people around the world who are constantly launching attacks on every system exposed to the Internet. Some of these millions of people know that they’re launching attacks, others have no idea that their devices have been compromised and are attacking on behalf of distant masters.

For those bulk attacks, we need bulk defenses. We need routers filtering traffic that then goes to the firewalls that then goes to the IPS. We need to limit the ports we leave exposed to the Internet, and for heaven's sake, don't allow your email server to be an open SMTP relay. If letting unauthorized users send email from your mail server hasn't been a problem in the past, it will be when the Brazilian spammer finds it and shuts your business down after sending upwards of ten million Portuguese-language spams.

And, yes, I speak from experience on that last point.

There are large numbers of unimaginative bad guys out there using yesterday's attack methods to see who has not yet learned the lessons of the past. Those bad guys are why we need perimeter defenses, anti-malware on every PC, and a proper patching process in place. But these things are more like border police than soldiers. They check everything on the way in to see if it should, or should not, continue on its journey. Much of the traffic is harmless, even desirable.

Militaries set up kill zones where anything that enters is fired upon and destroyed—and of course, we don't want to do that to customer orders or vendor invoices. We want to set up gateways where we can frisk the data entering the network and, even if it's dressed up as an order or an invoice, separate the threatening traffic from the desirable traffic. That is police work, in its essence.

There will also be threats from imaginative outsiders and insiders of all types. For those, we need to think of a Cold War metaphor: security as counterintelligence work.

When we think of the origins of modern computers, the counterintelligence metaphor makes even more sense. The first computers weren't Apples or IBMs, or even Ataris or Commodores. They were code-breaking machines, aerodynamics calculators, and nuclear equation solvers. They weren't built to do general-purpose functions or games; often, they were built to do top-secret things. The first computers belong more properly to the world of spies than they do to any other domain.

This also means that the job of keeping information on those computer systems secure also belongs to the world of spies more than to any other domain. Considering that there are computing systems from World War II that remain classified to this day (and that we know we don’t know much at all about those systems), perhaps we should take a closer look at the way spies operate, both in trying to access information and in protecting critical information from unauthorized access.

This is where we must divorce our thinking from what popular culture informs us about spycraft and cybersecurity. People on both sides are just that: people. Attackers have to check their code and squint at their screens and correct syntax errors, just like the rest of us. Although information can travel at the speed of light, less latency for the medium of transmission, actual cyberattacks typically take a great deal of preparation time, reconnaissance work, and gradual penetration in order to succeed. That’s not the stuff of good television or movies to most audiences, so James Bond steps in to liven things up.

At this point, I want to draw the line between brute criminal activity and targeted cyberespionage. The brute criminal activity is in the form of ransomware and phishing where the criminal doesn’t care at all about his or her target, only about said target’s money or other resources. Most of these attacks arrive in bulk, are known attack vectors, and can be dealt with by keeping perimeter defenses up to date and all information systems current on their patches and service packs. These are not imaginative attacks, they are wholesale ones—and it doesn’t take much imagination to deal with them.

Understanding—and Preparing for—Cyberespionage

For the rest of this essay, I want to focus on targeted cyberespionage. Some effort goes into this work. Instead of a random person calling up from “Windows Technical Support” and asking for your credit card number so he or she can repair your unbroken PC, these people can instead look up personal information about a target and then use that information to create an approach that’s more likely to have a profitable effect. For example, impersonating a traveling executive requesting a large amount of money to assist him in his business work. Another example would be creating a website that purports to deal with golfing, inviting executives who enjoy that sport to create an account there—and then using those account details elsewhere, in the hope that those credentials are the same as the ones the executives use for financial and business functions.

Targeted cyberespionage can go deep: including theft of company secrets, tracking individuals’ activities, sabotage of data and/or machinery, manipulation of information provided to investors, and even blackmail and worse. Unlike the brute criminal activity that is looking to profit from attacking anyone, targeted work is looking to profit from attacking a specific person or system—which means the attack will not be something unmodified, directly off the shelf. It may start that way, but it will be personalized or specialized as needed to improve its chances of success.

The story of how Britain broke German military codes in World War II is familiar enough that many people use it as an illustrative example of how a targeted attack is properly run, as well as what undermines such an attack. The British wanted to know what the Germans were doing with their military resources, but being at war, the British could not simply ask the Germans, "Beg your pardon, but could you please be good chaps and keep us informed of your troop and ship movements?" Because the Germans kept tight security around the machines that encrypted their messages, sending in a spy to, say, impersonate an officer and then steal such a machine wasn't very promising, either.

Besides, the French had already done that and shared that information with the Polish, who then also shared their groundbreaking work with the British. This brings up a pillar of cyberdefense: ***Share information with one's colleagues.*** Some of the best cyberdefense conversations begin with, "Say, this looks odd," "Can you take a look at this," and, my personal favorite, "Huh, that's funny." Other eyes looking at the problem mean other minds thinking about it, and we can leverage the wisdom of crowds—sorry for the cliché, but it explains perfectly how humans can work best when solving problems together. So I'll say it again: ***Share information with one's colleagues.***

The next thing the British needed to do was to monitor German radio signals. All of them. This is the second pillar of cyberdefense: ***Gather information. All of it.*** When I taught, I had students ask me how they would use what I was teaching in real life. I responded, "If you don't learn it, there's no way you could use it in real life. Be prepared." Same principle applies here.

The next pillar is: ***Analyze information for patterns and breaks in patterns.*** Patterns tell us what is to be expected. When the British studied German radio traffic, they learned a few things simply from the frequency of messages and their sources. That metadata could help to indicate where a major military operation was about to happen. That was nice, but even better was the day that a German radio operator neglected to follow proper procedure and took a short cut—a break in a pattern that allowed the British to jump at a chance to improve their code-breaking effort.

For their part, the Germans had suspicions that their codes might be breakable, but did not think that anyone would put in the effort required to actually do so. They underestimated their attackers, something very easy to do today, when computing power is cheap and getting cheaper by the day. Which brings us to pillar four: ***Your attackers are amassing resources to compromise your defenses.*** Brute attackers will attack and, if they fail or the attack is too hard, move on to the next target. Imaginative attackers will not move on because they want something specific that can't be had anywhere else. To get that something specific, they will do just about anything in order to get it. Had the Germans taken an additional step of improving their encryption security, they could have forced the British to start all over again in their efforts to break the German codes. The British would have increased their efforts, but any advantage enjoyed from a broken code would be short-lived with a policy to always increase the security of encryption. Not knowing what exactly one's enemies are attacking, one has to assume that anything that can and will be attacked—so efforts to protect infrastructure should be widespread.

Let me emphasize and clarify that last point. We do not strengthen everything all at the same time, but we do strengthen everything, in turn, in its own time. Consider a door to your home or apartment. Let's say you hear that robbers have a skeleton key for the kind of lock you've got on your door. A wise person would maybe plan a weekend project to replace that lock, and very soon. Then you hear robbers have started using tools to cut away the wooden door around the lock. A wise person then plans to replace the wooden door with a steel door. At that stage, you could probably guess that robbers will stop attacking doors, so maybe you also become proactive and look into securing your windows—actual windows, not the operating system—your patio door, maybe even your chimney. If you hear of tunneling attacks, maybe you purchase a seismic sensor that will dial the police if it detects sustained digging near your home. Maybe you do all these things, but you do each one in turn, not all at once. When deciding which areas you'll focus on securing next, you ask yourself how you'd break in yourself. The things you would try first are the ones to secure first. Then look for other areas that can be made more secure.

As it was, the Germans did make improvements in their Enigma codes and the British would then attack those, as well. This is the fifth and final pillar: ***Cybersecurity has no "happy ever after" ending. There is always another measure and there is always another countermeasure.*** There was no one day that saw the breaking of Enigma, once and for all, leaving the British as masters of all their enemies' communications. There was no one day when the Germans assembled an unbreakable code. Or, rather, the day the British broke the Enigma code for the last time, the Germans were months away from defeat. After that, the British had a new enemy whose codes they desired to break: the Russians.

Assembling these pillars, we can see them as a framework to support strategies, policies, and technology selections for cyberdefense.

1. *Share information with one's colleagues.*
2. *Gather information. All of it.*
3. *Analyze information for patterns and breaks in patterns.*
4. *Your attackers are amassing resources to compromise your defenses.*
5. *Cybersecurity has no "happy ever after" ending. There is always another measure and there is always another countermeasure.*

Cyberdefense specifics will change with the times: what was great encryption for 1917 is likely insufficient for 2017. However, the need for encryption—along with the need for physical security, information gathering, and data analysis—remains constant. The pillars of cyberdefense reflect the broad constants, not the specifics that change with the times.

The pillars also go contrary to the workings of most companies and bureaucracies. These groups can be very territorial. Different groups can view requests to share information and analysis as an erosion of their power or authority. Diverting resources to security means less budget for other hungry departments. Gathering information can be seen as contrary to the culture of the organization. Worst, the fact that cybersecurity is never-ending and always-escalating can make some managers or executives believe that cybersecurity is a lost cause.

To that I say: If cybersecurity is a lost cause, then why not publish all of one's customer data, sales leads, business processes, and proprietary information? And if the reaction is, "I can't do that! I'd go out of business!" then one has to face the fact that the cyberstuff needs to be secure—and that means investing in cyberdefense and creating a corporate culture that's conducive to security.

Teach people about what they should and should not say and whom they should and should not say those things to. Encourage employees to share information with each other and to report anomalies. Hire professionals who can analyze information and treat them well so they don't wander off. Keep patches up to date and use security measures to help improve productivity by reducing system downtime. Remain vigilant and encourage people to ask questions.

When I look at how other security organizations have operated, the most effective ones show that they've embraced the five pillars. Most have no need to send out investigators to dig up leads: they arrive in the form of people making reports of suspicious activity. When people believe that when they see something, they should say something, they come forward and report the unusual. Investigators then respond to the mass of volunteered information, weeding out anomalies with an easy explanation and any reports submitted to get back at another employee, and then what remains could lead to something big.

They then take those remaining leads and check with other groups and see if anything correlates or raises an alarm. Supervisors then make decisions on what to do with that information. Frequently, the best course of action is to quietly keep gathering more information, as a sudden move can result in alerting the attackers that they've been discovered, causing them to change their attack plan—and make it even more difficult to detect. Once enough information is gathered, the supervisors can direct an operation to shut down the attack in a way that catches as many attackers as possible, along with preventing the destruction of evidence. Then it's back to gathering information to detect the next attack.

What, then, would a strong cybersecurity organization look like? I'll illustrate an example for a medium- to large-sized company, adding the caveat that of course, your particular enterprise may have different needs.

The security team should be cross-disciplinary and maintain many contacts within many departments. There should not be a network security person who works completely independently and without knowledge of who’s responsible for application security. Security staff should be in communication with each other on a regular basis, as well as with their peers in their specialties. People from client, server, extranet, cloud, and physical security groups should be part of those communications, as well. And these discussions need to be not just at a managerial, director, or executive level: the engineers close to the actual operations of the company need to be talking with each other regularly and freely.

Each security engineer needs to have access to a security event information management (SEIM) system and spend some time of each working day just messing around with it, to see what correlates and what looks unusual. Don’t count on security vendors for alerts—targeted attackers are doing things that, if all goes according to plan, the vendor won’t notice. Rather than relying strictly on software, human intelligence and instinct are also valuable security tools.

At the same time, have information sensors everywhere, and get them talking to each other. (Here’s where I must use some jargon, so I invite the reader to investigate any terms he or she is not familiar with.) Get SPAN port aggregators and feed information to NetFlow monitors and NAC systems. Have an agent on each PC, Mac, and Linux box that can report on anything unusual happening. Tune your IPS systems to generate alerts on the weird stuff and keep an eye on what’s going on with your DNS traffic. In many firms, all those sensors will report into the SEIM, so it’s vital to find ways to have that SEIM generate alerts on certain things that can then correlate in actions taken within the environment. Does it matter if the NetFlow monitor or the IPS found a botnet controller on your office network? No, so long as the message sent by either of those systems to the SEIM triggers the NAC system to shut down the network connection for that controller.

From a policy perspective, the security team has to have permission to make mistakes—but be expected to learn from them. The security team should also have the authority to point out things that should be fixed immediately, and the culture should be that fixing those things has higher priority than the next code or product release.

When done best, security asks that corporate officers play a long game. Looking to goose numbers for the next quarterly report makes casualties of good security practices, tools, and people. Good security demands the retention of trained, experienced people, maintaining good tools, and looking ahead years in the future, when things may not be going so well. It is said that the bad thing about good times is that they eventually come to an end. Security is here to remind us all that the good thing about bad times is that they also eventually come to an end—so there is a valid purpose in fighting the good fight.

For companies with very immature or no security that crow with pride when a security vendor's demo doesn't turn up any issues, I have nothing but words of caution. True security does not rest on a single product or person. Gather enough information and begin to really ask some tough questions about your security set-up, and you'll soon see problems aplenty.

If we take another look at the intelligence community, we see that the most likely places for intrigue are directly under the noses of the most powerful officers and executives. When the U.S. intelligence community fought against Soviet spies in the Cold War, they didn't send planes full of agents to the USSR to round up suspects; they looked for spies in the USA itself, particularly in sensitive locations in both government and industry. Likewise, the Soviets searched for U.S. spies within their own top echelons, where a spy could do the most damage. It was not enough to use only one method to search for spies: perhaps all of a spy's associates would vouch for his or her loyalty, but a traffic analysis might reveal that the person is sending radio transmissions at odd hours of the day and night.

I recently watched a training film for OSS agents from World War II. It showed that one of the easiest ways for an agent to be noticed was to do something unusual—and those unusual things could be as mundane as having the wrong cut of suit or using grooming products not available to locals or using a knife and fork differently from everyone else.

For a 1960s training manual for U.S. intelligence agents, a magician was consulted to offer tips on using sleight of hand and misdirection for espionage. Above all, the magician stressed that all actions need to appear natural. Magicians, spies, and hackers alike succeed if their tricks look like completely unremarkable actions.

This is how cyberattackers after intellectual property and the like operate. They don't want to take down the network or compromise workstations. Quite the contrary, their success depends upon that coveted 99.999% uptime so that their actions, made to appear completely unremarkable, will succeed. That's why data collection, sharing, and analysis are so vital in cyberdefense. The more things you examine, the more likely you'll spot the one anomaly the attacker could not disguise.

Expect the attacks. Expect them to be constant, as well as constantly changing. Keep tools, processes, and staff up to date and well supplied so they can deal with those attacks. Use information in order to protect your information. You are not fighting a conventional enemy, but someone whose profession is a logical extension of the espionage community. You do not need generals to fight the cyberwars: you need spymasters and border police.

1. *Share information with one's colleagues.*
2. *Gather information. All of it.*
3. *Analyze information for patterns and breaks in patterns.*
4. *Your attackers are amassing resources to compromise your defenses.*
5. *Cybersecurity has no "happy ever after" ending. There is always another measure and there is always another countermeasure.*

Dean Webb *is a Dallas-based computer and network security specialist. He has started a career in IT twice, and watched it develop rapidly into a very satisfying line of work each time. As a former teacher, he enjoys passing on useful information to anyone willing to hear it. To hear more from Dean, check out Networking-Forums.com or his Peerlyst profile*.

Chapter Three

Driving Effective Security with Metrics

By Anthony Noblett

What are Security Metrics?

Security metrics are the output of measurement of a security control or security activity. In the case of IT security, many things can be measured, including people, processes, and operations. Security metrics are usually not interchangeable between companies and situations, which seems to make the concept more difficult. The trick is starting with a clear goal and an understanding of the results you wish to accomplish with your security metrics.

Defining measurement seems to be a difficult concept in security, since the most commonly available measurements can be difficult to get exact. I'd recommend using this standard definition of measurement: A quantitatively expressed reduction of uncertainty based on one or more observations. That definition deals with the security realities of a measurement not being infinitely precise, as well as the fact that empirical methods may not be practical to use.

Security professionals were initially held accountable for protecting company assets, but as security has become both more complex and widespread, they are also expected to contribute to an enterprise's financial and competitive success. This requires a broad view of security metrics and measurement.

Security metrics are not universal, and what works for one company and situation may not work for another company or situation. Metrics should be designed to the situation and will likely be adapted and modified by the CISO over time. The metrics under measurement should, however, fit some basic tenants that we will discuss in this chapter.

Good Security Metrics

In any situation, useful metrics must meet basic requirements, whether for security or for any business need. The metric must be:

- Necessary to meet a business requirement
    - Contextually specific to the requirement
- Consistently measured
    - Consistent over time
    - In a consistent unit of measure
- Cheap to obtain
    - The resource cost of producing the metric must be less than the cost of remediation to eliminate the need for the metric
- Quantifiable
    - A number, percentage, or a statistical measure

In addition to these basic requirements, good security metrics enable more process-oriented activities such as:

- Communication of performance
- Performance improvement
- IT controls testing
- Problem diagnosis
- Accountability (personal and departmental)
- Resource allocation
- Compliance
- Use of industry benchmarks

Some examples of security metrics are:

- Percentage of unpatched security vulnerabilities on critical systems
- Percent of endpoints with up-to-date protection
- Percent of policies, procedures, and standards created and implemented
- Industry maturity benchmarks to standard frameworks

- Time to remediation
- Endpoint configuration standardization
- Number of security anomalies detected by automation
- Compliance to change control process: normal vs. emergency
- Percent improvement in phishing resistance

Meaningful Security Metrics

How do we select meaningful metrics? Start by having a clear goal that the metric informs. The best security metrics are SMART: specific, measurable, attainable, repeatable, and time-dependent. To get these metrics, one method used in computer science is called the goal question metric (GQM). GQM works extremely well, in part because it is straightforward and clear and leads to meaningful metrics with little ambiguity.

Using the GQM method, a top-down alignment with business goals is obtained. This approach counters the tendency of most InfoSec professionals to start with a bottom-up approach. The problem with a bottom-up approach in InfoSec is the systems, tools, and networks common in security influence that bottoms-up approach, making the metrics less meaningful to the business.

Example of GQM

Let’s walk through an example of deriving metrics using the GQM approach:

Goal

A good goal must be specific, with criteria for both success and failure. Also a goal should be limited with a defined and bounded scope. A goal must be attainable and verifiable within a specific context—and most important of all, a goal must be documented, accepted, and tracked.

- Evaluation of the company’s compliance to the requirements of PCI DSS 3.2 by comparing the company knowledge and activities to the PCI DSS 3.2 guidance provided by PCI DSS 3.2 from the perspective of the PCI Qualified Security Assessor (QSA).

Question

What is the specific question to be answered by the metric? In this example, it is requirement 3.1 of the PCI DSS requirements.

- Does the company protect stored cardholder data?
    - Limit data storage amount and retention time?
    - Specify retention requirements for cardholder data?
    - Provide secure processes for deletion of cardholder data?
    - Provide a quarterly process to sweep for and delete cardholder data that may have exceeded retention time?

Metric

Examining the questions, what are the specific things, actions, or reactions that can be measured to answer these questions? In this case, the guidance from the PCI Council to meet requirement 3.1 are spelled out:

- Measure the data-storage size limit on cardholder data
- Measure the cardholder data-retention limit and reason for retention
- Verify and measure the deletion of cardholder data process being run
- Sample to verify the use of a process for sweeping for cardholder data-deletion when retention has been exceeded

This example, if worked all the way through the PCI DSS 3.2, will be detailed and wouldn't be practical, even with only one compliance requirement. Companies have multiple overlays of compliance requirements, which lead to the use of a common framework. A best practice is to build roll-ups of questions to reduce the detail, while still providing meaningful metrics.

Frameworks

Frameworks provide as much coverage as possible while still providing a reasonable operational tool. By "reasonable operational tool," I mean that the framework has to make sense to the person managing the security operation, and at a level that is operationally meaningful. Framework selection can be a religious argument, so in this case the discussion is focused on metrics. Security professionals often use specific frameworks for specific reasons. Those reasons are rooted in outside influences such as audits, compliance, or management demand. Use the framework that makes sense to you as the security professional managing the operation. Frameworks have been mapped to each other over the last several years, so if the selection is not what someone on the outside wants, it's pretty easy to recast to another framework.

In the U.S., the National Institute of Standards and Technology (NIST) has created what is called the NIST Cyber Security Framework (CSF). It has gained tremendous traction in a very short time due to endorsements from all of the major security standards organizations and more important, the National Association of Corporate Directors (NACD). The top three levels of the NIST CSF are the most important to a security metrics discussion.

As a security professional, it is important to pick a framework and stick with it in the operation that you are managing. Personal experience has been that the NIST CSF at level 2 works best to manage security organizations, level 1 works best for the C-suite and corporate boards, and level 3 for the auditors. Another framework that is widely used is called the Center for Internet Security (CIS) Critical Security Controls Framework (previously called the SANS Critical Security Controls Framework). This is best used at the control level to manage the security organization. The system level is not easily understood by the C-suite, which makes it a bit more work come reporting time. Both the NIST CSF and the CIS CSC are easily translated to compliance requirements and are well understood by most auditors.

Operational Metrics

Real-life operational metrics are a combination of numbers, percentages, security maturity, and organizational benchmarks. By taking the examples used earlier in this chapter, I can explain a bit better.

Percentage of unpatched security vulnerabilities on critical systems

This metric relies on knowledge of and control of critical systems. For example critical systems would be the servers that run the e-commerce site of a retailer. Critical servers include the Web server(s), application server(s), database server(s), connections to the point of sale back-end, and marketing analytics server/service.

These systems typically run with very high up-time and can be difficult to patch. They also can be sensitive to patch-induced breakage, and must be tested prior to patching the production environment. The number of servers requiring critical patches divided by the number of total critical servers is the measurement we are after.

Percent of endpoints with up-to-date protection

This measurement is the number of endpoints that have communicated with the central console of the anti-virus system within the last 24 hours, divided by the total number of endpoints. It should be taken on both the traditional AV system and the advanced malware prevention system.

This metric is also an indicator of issues in the systems management software (SCCM, Altiris, KACE, etc.) and should be used to work with the endpoint management team to increase check-in coverage of endpoints. Often it also is an indication of network visibility and segmentation issues in operations, and is highly valued by the infrastructure team.

Industry Maturity Benchmarks

This powerful metric is where use of a framework is mandatory. The framework is used with a combination of a CMMI rating with relative risk, likelihood of occurrence, and impact of an occurrence to provide a good measurement of where the company is with respect to other companies in its industry. Industry comparisons are available from the Information Sharing and Analysis Centers (ISAC) in the U.S., from the Big Four accounting firms, and from large value-added resellers (VARs).

In developing this rating system, the relationships of risk, likelihood, threat, and impact come directly from the NIST CSF assessment template. The definitions and relationships from that framework are shown below.

Maturity (Software Engineering Institute's CMMI rating)

Modified for security using the concepts in the paper *Considering the Case for Security Content in CMMI*

Number	Rating	Description
5	Highly Mature	Focus is on process improvement
4	Mature	Processes are measured and controlled
3	Somewhat Mature	Processes characterized for the organization and is proactive
2	Immature	Processes characterized for projects and is often reactive
1	Highly Immature	Processes unpredictable, poorly controlled, and reactive

Relative Risk

- Low
- Medium

- High

Likelihood

The likelihood of an occurrence

Likelihood	Description
High	The capability of the threat is significant, and compensating controls to reduce the probability of vulnerability exploitation are insufficient
Medium	The capability of the threat is medium, and implemented compensating controls lessen the probability of vulnerability exploitation
Low	The capability of the threat is limited, and compensating controls are in place that effectively reduce the probability of vulnerability exploitation

Impact

Definitions of the impact on the organization

Likelihood	Description
High	The capability of the threat is significant, and compensating controls to reduce the probability of vulnerability exploitation are insufficient
Medium	The capability of the threat is medium, and implemented compensating controls lessen the probability of vulnerability exploitation

Low	The capability of the threat is limited, and compensating controls are in place that effectively reduce the probability of vulnerability exploitation

Relationships between factors

The security team develops the relationship between the maturity, risk, likelihood, and impact factors. The relationships should be primarily multiplication with some constants. These relationships vary between businesses depending on the industry, so an exact relationship cannot be shown here.

Endpoint configuration standardization

This measurement is the percentage of endpoints, which are running OS images un-modified from the standard image. Changes to the endpoint image should require formal change management and approval by security. Images should be targeted to standard configurations such as the Center for Internet Security benchmarks. This measurement should be low if the image is correctly configured.

Number of anomalies detected by automation

These measurements come from the Security Operation Center (SOC) and show the verified anomalies that have been found by the SIEM/IDS/vulnerability processes. It is important that the measurement is of verified anomalies, and they are not declared incidents until they meet the management-agreed definition of an incident. Trends are important in this case, and indicators should be customized to the vertical market and the company.

Percent improvement in phishing resistance

An increase in the percentage of users able to distinguish between a phishing email and a business email is desirable, and should be measured. This measurement is a good indicator of when modifications are needed to the security-awareness program, or if the program needs to be given to users more often. This measurement can also be used to add some fun to security by organizing friendly competitions.

Audience

The critical question for all security metrics is “Who is your audience?” As mentioned earlier, for a metric to be meaningful there must be a business context and it must be useful to the business. Different levels of the business have different contexts—and they view security metrics differently.

Board of directors

The boards of most companies have some basic interests in information security. The four most common questions they want answered are: The four most common questions they want answered are: The four most common questions they want answered are:

- Are we secure enough?

- How do we compare to our competitors in information security?

- Does information security help us sell more and make more profit?

- What investments do we need in information security?

These questions require coarse-grained metrics, and must be answered clearly, with no ambiguity. Too many technical details and definitions can cause poor understanding and loss of credibility with boards. Metrics that work with this audience are maturity ratings compared to competition, increase in readiness for security breaches, compliance status, and work won or products sold due to the company’s security posture. The last one is hard to measure, but critical to the security program. The CISO must be able to show that security has helped win business and increase sales.

C-suite

The C-suite wants answers to different questions. Examples of their questions are:

- What is the status of current and upcoming security projects?

- Are we going to make our compliance-related goals?

- What is the overall value of the current security program?

- How does security mesh with the rest of our business goals?

Examples of metrics that matter in these cases are:

- Status of current security projects and the upcoming spend for out-year projects
- Status of the yearly compliance process, such as the Report on Compliance (ROC)
- The percentages of security spend as part of the overall IT budget
- Security enablement of the replacement rebuild of the current ERP system

Auditors

Auditors are the people security practitioners spend a good portion of their time thinking about. Auditors have the most detailed requirements for metrics, and they include internal auditors, compliance auditors, and external auditors. The level of metrics given in the earlier example gives you some idea of where an auditor lives. If you plan for audit-level detail, all lower detail metrics, including board level and C-suite, can be derived from these metrics.

- Internal audits. The internal auditors focus on questions like, Did we do what we said we would do with respect to security? Typically that means observations and tests of policy, procedures, and standards compliance. And testing of change control and documentation compliance.
- Compliance audits. Examples are the PCI DSS QSA audits, the FFIEC banking audit, the DoD FISMA or FedRAMP audits. These audits require detailed evidence that show that compliance is being maintained. The GQM approach will provide this information consistently and reliably when designed to meet this goal.
- External audits. These audits are the Sarbanes-Oxley audits for public companies and the AICPA SSAE 16 Service Operation Compliance (SOC) audits. Clear design of metrics using the GQM method will also provide the necessary detailed information. If properly designed, the metrics will yield information that can be used in both compliance and external audits.

References

IT Security Metrics: A Practical Framework for Measuring Security and Protecting Data. Lance Hayden PhD. CISSP, CISM: McGraw-Hill Education 2010.

Data Visibility: A Matter Of Perspective Joshua Goldfarb, DarkReading 8/10/15 UBM http://www.darkreading.com/analytics/data-visibility--a-matter-of-perspective/a/d-id/1321687?

Security Metrics: It's All Relative, DarkReading 6/9/15 UBM http://www.darkreading.com/analytics/security-metrics-its-all-relative/a/d-id/1320772?

A Guide to Effective Security Metrics 07/31/15 2014 Effective Security Metrics https://spaces.internet2.edu/display/2014infosecurityguide/Effective+Security+Metrics

Gathering Security Metrics and Reaping the Rewards, SANS Institute InfoSec Reading Room, Dan Rathbun 10/7/09 https://www.sans.org/reading-room/whitepapers/leadership/gathering-security-metrics-reaping-rewards-33234

A Guide to Security Metrics, SANS Institute InfoSec Reading Room, Shirley C Payne 6/19/06 https://www.sans.org/reading-room/whitepapers/auditing/guide-security-metrics-55

Security Metrics: What are you Measuring? The State of Security Tripwire Dwayne Melancon 6/19/12 https://www.tripwire.com/state-of-security/security-data-protection/security-metrics-what-are-you-measuring/

No One Cares About Your Security Metrics and You are to Blame, Gartner Blog Network Paul Proctor 8/11/2013, http://blogs.gartner.com/paul-proctor/2013/08/11/no-one-cares-about-your-security-metrics-and-you-are-to-blame/

CIS Critical Security Controls https://www.cisecurity.org/critical-controls.cfm

NIST Cyber Security Framework https://www.nist.gov/cyberframework

What's Your Security Maturity Level? https://krebsonsecurity.com/2015/04/whats-your-security-maturity-level/

How to Measure Anything in Cybersecurity Risk. Douglas Hubbard and Richard Seiersen, 2016, John Wiley & Sons.

***Anthony Noblett** is an experienced CISO and cybersecurity professional with deep experience in information security systems, governance risk and compliance, application security, and security in private and public clouds. To learn more about Tony, check out his profile on Peerlyst or LinkedIn.*

Chapter Four
A Security Compromise Lexicon
By Nicole Lamoureux

Sony Online Services, 2011. LinkedIn, 2012. Target, 2013. Yahoo, 2014. Anthem, 2015. FriendFinder, 2016. I could go on and on when it comes to listing organizations that have been breached over the years. It's not just big name brands either: Every single organization, small and large, is at risk from attackers.

In order to explain how a compromise may occur, I need to explain a few other things first. Organizations face two different types of threats, internal and external. An **internal threat** comes from an employee or an outside individual with privileged access to an organization's IT system, while an **external threat** comes from an individual or group outside of the organization seeking to gain inside access.

Internal threats fall under two categories: internal accidents and internal attacks. **Internal accidents** occur when security falls victim to human error. For example, an employee may leave confidential papers in a printer while grabbing a coffee—leaving time for someone to take a peek or worse, make copies—all without the employee knowing.

An **internal attack** is generated by malicious insiders. They are employees, contractors, or business partners with privileged access to an organization's IT systems who use that access to damage the company in some form. Sometimes they do this because they are disgruntled; sometimes they are seeking to profit on the black market. Malicious insiders can be difficult to detect if the proper security controls are not in place.

An **external accident** occurs when something external to the organization fails and affects the productivity of the company environment. Such an accident could be a huge thunderstorm knocking out a power grid and losing access to an off-site backup server.

An **external attack** is what most organizations seek to avoid—and the kind of compromise that's most likely to be reported in the media. These types of attacks occur when a powerful outside entity seeks to launch a distributed denial of service (DDoS) attack, manipulate data, or breach your network. And the unfortunate fact is that a highly motivated attacker with the time and resources can breach any network.

In the real world, these categories can overlap. Say an employee leaves his corporate laptop in a car overnight, and when he returns to the car the next morning, he notices the car has been broken into and the laptop has been stolen. There's actually both an internal and external threat in this situation: 1) the employee left the corporate laptop unattended, breaching policy, and 2) the corporate data on the now-stolen laptop can be read by an outside attacker.

What Happens When an Organization Is Compromised?

The areas of possible exposure can be summed up by the CIA triangle:

- There is a known breach of data in the network's **confidentiality**. The data was most likely exfiltrated to a public site like Pastebin to be sold off to the highest bidder. An example could be a breach of credit-card information from a company database.
- The data in place on the network has been manipulated and is no longer accurate and therefore the **integrity** has been compromised. This can be the hardest to detect if there are no data protection controls in place. An example of such an attack could be the redirection of funds for a banking website. A man-in-the-middle attack with a bank could easily result in a change in banking-account details, leaving the funds transferred to an account different from the one the sender intended to send the money to.
- There is a denial of a service occurring in the **availability** of an organization. For example, if a huge load of traffic hit a website that's not designated to handle that traffic load. This type of compromise is a common occurrence and can even be the result of an accident.

Types of Attackers

Corporations. Corporations have been known to breach one another's security boundaries to perform malicious acts, therefore gaining a competitive advantage. Some call this **corporate espionage**.

Nation states. Will often target other governments and private entities with a high level of technical sophistication to obtain foreign intelligence or cause destructive activities.

Hacktivists. Acting individually or as a group, they are often politically motivated and may target specific individuals or organizations to further their cause.

Cyberterrorists. Frequently targeting critical infrastructure and government groups, they are characterized by the use of violence to achieve their end goals.

Criminals. Highly motivated by the desire for money and profit, they are generally involved with fraudulent financial transactions.

Cyber fighters. Similar to hacktivists, a cyber fighter or cyber warrior is generally a nationally motivated citizen who acts on behalf of a political cause or against a political entity that threatens him or her.

Script kiddies. Young or inexperienced individuals who are in the process of learning to hack, script kiddies may work alone or with others, usually on actions such as code injection and DDoS attacks.

Online social engineers. Are frequently involved with cyberbullying, identity theft, and the collection of people’s private information.

Employees. Typically using low-tech methods and tools, former or dissatisfied employees are a high security risk. Even a well-intentioned employee may accidentally cause an incident, especially if proper security controls are not in place.

Malware—What is it?

Malware, also known as **malicious code**, is software designed to gain access to a target system, steal information from a device, or disrupt normal computer operations. Malware can target multiple components for a higher degree of maliciousness. Below are some of the common types of malware to be found in the wild:

Adware. Designed to present a user with advertisements, which are generally unwanted and may slow system performance.

Botnets. A botnet is a largely automated and widely distributed network of previously compromised computers that can be simultaneously controlled. These botnets, such as the Mirai botnet, are widely used in large-scale DDoS attacks.

Keylogger. This form of malware secretly records user keystrokes and, in some cases, even screen captures.

Ransomware. A class of malware that criminals use to extort money from a user by locking or encrypting data files until a ransom has been paid.

Rootkit. Hides malicious processes within the operating system and tries to prevent detection by security software.

Spyware. Malware that secretly gathers and collects information about a person or organization.

Trojan horse. A piece of malware that gains access to a system by hiding within a genuine application. It may also be a piece of software that claims to do one thing, but actually performs another action.

Virus. A virus can replicate itself and spread from one computer to another, but it requires user intervention or execution to replicate and/or cause damage.

Worm. When carrying out routines programmed by the payload, or malicious code, a worm can replicate itself to other computers and networks without any user interaction.

Other Attack Types You Should Know About

Advanced persistent threats. Complex and coordinated attacks directed towards a specific target. An enormous amount of time and research is put into this form of attack.

Backdoors. Regaining access into an already compromised system by using existing or newly installed software to enable remote access.

Brute force attack. Attempting all possible combinations of a password or encryption-key possibilities until the correct one has been found.

Buffer overflow. This attack affects the integrity of the data when a program or process tries to store more data in a buffer (temporary storage area) then it was intended to hold. Since a buffer can only hold a finite amount of data, the extra data overflows into adjacent buffers—corrupting or overwriting the data held within them.

Cross-site scripting (XSS). An injection-type attack in which malicious scripts are injected into trusted websites. An attack occurs when an attacker uses a Web application to send malicious code to a different end user. Validating user input prevents these attacks.

Denial of service (DoS). Generally refers to a single computer targeting a network device by flooding the target with requests for resources, disabling other legitimate users from accessing those resources.

Distributed denial of service (DDoS). A massive collection of computers, generally considered a botnet, used to overwhelm a target system or network and prevent legitimate users from accessing that system or network's resources.

Phishing. A type of email attack that attempts to convince a user that the originating user is someone they're not. The attacker has the intention of social engineering the user in order to obtain information.

Social engineering. An attempt to exploit social vulnerabilities to gain access to specific information and/or systems. It generally involves a "con" to trick others into divulging confidential information or opening malicious programs.

Spear phishing. A targeted social-engineering attack in which an attacker uses information gained about the user in order to convince that user of the attacker's assumed identity.

Spoofing. The faking of a transmission address in order to gain entry into a secure system.

Structured Query Language (SQL) injection. A SQL injection results from the failure of an application to appropriately validate its input.

Whaling. A social-engineering attack targeting an executive, in which the attacker masquerades as a trusted party to glean confidential information

Zero-day exploit. A new vulnerability that is exploited before the software creator is even aware of its existence.

***Nicole Lamoureux** is the principal of Nikovault Security, a consulting firm based in Winnipeg, Manitoba, Canada. She is passionate about technology and advocating for women in security, and frequently blogs about InfoSec topics on Peerlyst.*

Chapter Five
Building a Corporate Security Culture
By Dawid Balut

All my years in InfoSec have taught me that for security initiatives to be effective, security must be one of the core values of corporate culture. Security professionals can't achieve their greatness if they're not being actively supported by all stakeholders across the entire organization, and if other employees don't feel ownership over the organization's safety. Each time I joined organizations where security professionals wanted to do everything all by themselves, they failed miserably shortly after.

Fighting with a broken security culture without any support from the top leads to the burnout of InfoSec folks, and creates general anxiety and irritation within an organization.

So I'll share a list of activities I found to be the most effective and productive in my security career. Unfortunately, I've had to go through a painful path, but by sharing these ideas with you, I hope you will learn from my mistakes and avoid them in your career to become more effective without burning out your passion, health, and relationships with co-workers. All of the things I'm sharing are not abstract theories, but activities that were successfully executed by someone who got his hands dirty by applying ideas to real-life businesses.

Understanding these concepts will enable you to see the bigger picture and gain a richer point of view, but please see this chapter as a source of inspiration and hints, not a rigid set of rules. I'm giving you food for thought, which you'll need to thoroughly consume and adjust to your organization and your personality. Enjoy!

Start small

Take baby steps to show that security doesn't need to be tangled and complex. If you show people that it takes just three clicks to achieve a really good security posture, their mindset will change and they'll be eager to implement more of such hassle-free solutions. Do the things that have the biggest ROI and lowest cost of implementation, then steadily increase the complexity of security requirements.

The common mistake I’ve seen is that InfoSec professionals try to start out too big. They want to enforce all the possible rules as soon as possible or even better—all at once. While this approach may sound reasonable from a security perspective, it’s a complete disaster from a practical business POV and I haven’t ever seen it be successful.

Building security is tough, not because it’s complicated, but because it takes a lot of time, perseverance, and emotional work. If you’re joining an organization that’s a few years old and never had a security person/culture before, you must prepare yourself for the slow rollout of all the great ideas you have. People who were never taught to be security savvy will have a hard time adopting many changes at once—even if you have a reasonable justification for them. For example, when limiting access, do it in many small stages, otherwise you may outrage people when they lose access to most things they used to use freely for years.

The best way to build credibility and get immediate results without irritating people is to start with subtle changes like showing the value of strong passwords, password managers, two-factor authentication, antivirus and regular software updates—all of which, adopted across the board, will result in a good security baseline.

Start early

The earlier you start, the more effective you’re going to be, for two main reasons. One is that people won’t even have a chance to form bad habits if good security practices are expected from the start. And second, it’s more expensive to do design changes and refactoring of a finished product.

I recommend that all-sized businesses seek the help of security consultant as early as possible. A few hours of consultancy won’t ruin your budget, but can give you a baseline upon which you can build your security program and avoid a lot of refactoring/breach costs in the future. Chances are that you know someone passionate about security who’ll be more than happy to support you free of charge and ensure your products are robust, so reach out to your social circles and ask for help.

Set common goals with management and executives

Unfortunately, we’re still a long ways off from a time when security will be included in quality-assurance processes by default, and everyone will be aware of the potential consequences of security negligence. Especially in start-ups and SMBs, very often middle management isn’t held responsible for product security, and the only thing they’re rewarded for is if the product is shipped.

If you don’t start from the top of an organization’s hierarchy, it’s unlikely you’ll succeed with your security initiatives, because engineers don’t like to step out and do things their managers don’t want them to spend time on.

Before you start working with engineers, make sure you have the support of executives. To get that, learn about the business objectives of your company, as well as management’s key focus points, then tailor your security plans accordingly. It’s hard to offer general recommendations here, because each organization and each exec is different, so you need to approach them on individual basis.

Senior management advocate for a healthy security culture, otherwise it’s a Sisyphean task to do all the things from the bottom up. No leadership, no time, no budget, no resources = no security improvement.

Everyone is a target

This is a problem I often run into while working with start-ups and SMBs, which tend to believe that they’re too small to become a target. The truth is actually the reverse: hackers and script kiddies come after the easiest targets and immediate profit first, so they’re very likely to attack organizations with a weak security posture.

Management needs to also understand that while big organizations can survive a security breach, small ones can’t afford them because of PR reasons. If a business providing enterprise solutions has a stable position in the market and great product, most customers will stay because it’s expensive to switch a whole enterprise to another solution. But if you’re a small startup that has been compromised, it’ll get overblown in social media by competitors—then you’re finished, at least PR-wise.

This is a really important message to convey because recently I’ve seen many articles saying that it’s cheaper to get hacked than to secure an organization—an idea that’s nonsense, and makes it even harder to raise execs’ security awareness. Instead, remind executives that basic security isn’t that expensive, and ensure that everyone in the organization understands business risk management, including the dangers coming from social media scandals. Offer solid perspective on why security breaches bring different results to different organizations.

You can earn some love from your marketing and sales people if they learn that you’re protecting the business in ways that will make their job easier. For instance, if you prevent the organization from being hacked, they won’t need to explain what went wrong to customers and prospects—and convince them that you’re doing much better nowadays.

Establish authority as soon as possible

Security is an executive-level issue, so you must be in position to influence everyone else in the organization. I’ve wasted far too much time on back-and-forth discussions about why something must be done this way, and not other way around, because I was not given enough authority. Without it, I had to escalate matters up through many ranks.

If you establish your authority as early as possible, you’ll save yourself lots of anxiety and frustration. Fighting with management will suck out your soul after a few years, and I don’t want you to burn out fighting unnecessary battles.

Simply said, you need to be in power on a management level to make a difference and be productive. If you’re on the lowest rungs of an organization chart, you’ll have a hard time working with non-security-aware management, who tend to see security just as something that slows down the development process—and their prime objective is shipping working product out on time.

At all cost, avoid confusion and FUD

Credibility is something you’re building from day one to the last day of your career. Even if you’re a great industry expert, you still need to build your internal reputation from the ground up by working nicely with people in your organization.

One very important thing you need to learn is how to weigh your words carefully, especially while talking about severe security flaws and vulnerabilities you've discovered. You may have great intentions, but if you speak in unclear terms and dramatize too much, you'll get the opposite of the results you're after.

Aim to look like you're relaxed and have everything under control—otherwise people may perceive you as someone who doesn't understand the business and wants to slow everything down to build a security fortress.

Even when rolling out common-sense security initiatives, people may react negatively if you have even a slightly aggressive tone, and they may dismiss your suggestions. People also react badly to perceived panic, so sometimes it's better to underrate the issue you're reporting so they accept it without anxiety. Once you've built credibility as a smart security leader who understands both business and risk management, you can start being more expressive and authentic. Yes, modulating your tone and minimizing your "asks" mean that you'll probably get less technical work done at the beginning, but building credibility pays off in the long run.

Another truth is that if you make too many mistakes—whether in implementation or by not satisfactorily answering people's questions—people may stop respecting you and your expertise, and that's a tough situation to deal with.

If someone in the organization raises a question you can't answer, admit your knowledge gap, go out and get the information you need, and then get back to the questioner with the information they need. Never let your ego lead you to make things up, because if people see through you, you have more to lose than to gain.

Make it clear that security is a cost like any other

Security shouldn't be seen as necessary evil and an "addition" to product development. Instead, it's a part of the systems development life cycle (SDLC), and an important component of quality assurance. In my experience, management changes its attitude toward spending on security when it thinks about security as a regular cost of software development, not as a no-ROI-time-waster that slows product development.

Try to establish how much time is going to be dedicated to security improvements and fixes. For example, how many hours in each product-development sprint will be spent on security, and how much free bandwidth does engineering have for unexpected security patching. It's hard—in fact, in most organizations, it's impossible—to stop all business activities and focus entirely on security for a few weeks so you can fix all the vulnerabilities you've identified. So I recommend you go with an approach that specifies the percentage of resources that will be spent on security in each product release/sprint.

Build secure SDLC

Security should be initiated in the earliest design phase of SDLC, because the old practice that I've seen everywhere—"Let's build it, then throw it at the security team"—doesn't work well, and it's certainly not cost effective. While it was more practical in the past because applications were smaller and less complex, nowadays products tend to be so big, it's hard for security teams to do all their magic and secure the product in just a few days before it hits production. Instead, security pros should get involved during the product-design phase and keep an eye on things throughout the whole development process. The latter can be accomplished by plugging security automation into the continuous development process, so you know when there is something new and have tests running continuously. Everyone needs to be aware that security testing takes quite a lot of time, and it must be included in release-schedule planning. I personally like to jump in with final pen tests when the quality assurance (QA) team is doing their testing. Asking for separate time after QA testing would really slow the shipping process, which is something we in security should try to avoid. The #1 rule of effective security is to do your best to never slow anyone and anything down.

If people see you all the time during design discussions, they'll organically learn you're needed—and they'll be more likely to let you know whenever there's something coming up that you need to be aware of.

If you'd like more of my tips on building a corporate security culture, click here to keep reading.

Dawid Bałut *is a security architect at a Silicon Valley security start-up and a founder of InfoSec Remedy, where he shares his knowledge to help other start-ups and SMBs build effective security from the ground up. He also writes on leadership and effective management on his blog. If you want to contact him, you can do so through his Peerlyst profile or LinkedIn.*

Chapter Six

Why People Are Your Most Important Security Asset

By Darrell Drystek

The classroom was filled to capacity with young and mostly eager minds when the instructor walked in. He was a tall, portly man carrying a weathered brown leather briefcase. He ceremoniously dropped it on his desk to silence the room, turned, picked up a piece of chalk and scrawled four big block letters on the blackboard: "GIGO." Slowly, he turned around to face the class, then boomed "It means 'Garbage In, Garbage Out' and it is the single most important thing to remember from this course—and for all of you to keep in mind in every other course you will take in this program of studies!"

More than forty years have passed since that first day of Introduction to Data Processing, and although I can no longer recall his name, my instructor's brash cautionary introduction into the world of systems analysis and design remains with me to this very day. Just in case you may be as green as we were as young students back then, let me elaborate on the GIGO concept: People design, implement, and operate technology. People design, manage, and operate business processes. Ergo, if garbage is the reason a system or a process fails, then it is a problem that only people can solve.

People are a part of every business process, and the most vital part of every information system that supports a business process. You may have designed the very best process or system in the world, but it is the action or inaction of people that will ultimately determine whether you succeed or fail. The same holds true for designing, implementing, and operating a truly effective security program. Truly effective security requires building bridges, not just fences—and that is what this chapter is all about.

The Uncomfortable Truth About People and Security

Security is not a self-serving process unto itself. It is a product/service developed and implemented to support a business need, which at the core is to serve and protect people from the unwanted actions of (other) people.

Technologies and methodologies will come and go. The password and the padlock are simple and familiar security controls that have been used to control physical access to assets since the days of the Roman Empire. We continue to deploy modern versions of these "ancient" access controls today because these can be appropriate and made effective for certain risk scenarios. However, whether our goal is to control access to the Roman Senate or a modern-day data center, it’s people who decide the design of access controls, as well as how the controls are deployed and used. People are the only constant in any security risk equation and the key ingredient for a successful security program.

Security processes always add some degree of overhead to an organization's operational processes. So, obtaining “buy-in”—support from the people affected—is absolutely critical for security processes to be embraced and used effectively. Your chances of garnering support improve greatly when security processes are perceived as appropriate in terms of the actual protection requirement.

Appropriate security is a balance of cost, safety, and usability, after factoring in applicable regulatory and/or legislative compliance requirements. Exactly what may be defined as “appropriate” by any one entity or person will depend on the specific tolerance for residual risk. Also, risk tolerance levels tend to morph along with maturity and experience, in both individuals and organizations. For example, the risk tolerance level is usually much different for a start-up than a Fortune 500 enterprise.

People want and expect to be secure but they will only truly support the additional overhead of security processes when they perceive them to be of value. And where people feel that they have a personal stake in a cause, they tend to be much more receptive and supportive. Don't just simply apprise people of their individual security responsibilities: explain why the requirements are appropriate and beneficial and encourage suggestions for improvement. As Benjamin Franklin famously said "Tell me and I forget. Teach me and I remember. Involve me and I learn."

Good Security Governance Is the Key to Building Relationships

The vast majority of security breaches are not caused by dastardly highly skilled hackers employed by criminal gangs or moon-faced dictators, smashing through firewalls like unstoppable virtual Rambos. Most security incidents and data loss result from sloth or apathy: employees not following security policies and procedures, employees poorly trained in safe data-handling practices, employees falling prey to social engineering scams.

Organizations spend millions on technical controls, but the true root cause of every security breach can be traced to a gap or gaffe in governance. Poor governance is a “people” or “management” problem. Some common failure points—governance gaps or gaffes—are:

- Absence of clear and relevant security policies and procedures.
- Data classification not done, poorly done, or not kept up-to-date.
- Poorly crafted or inappropriate security policies and procedures.
- Inadequate training of employees in safe data-handling practices.
- Assigned access rights that are greater than or not equal to the actual job role/requirement.
- Access rights assigned, then not reviewed, approved or adjusted on a regular timely basis.
- Security programs that are not sufficiently enabled to rapidly respond to morphing threats.
- Absence of robust, disciplined change-control procedures.
- Lack of support from the entity's leaders in enforcing employee compliance with controls.

Good governance is fundamental for effective security. Good governance is not delivered through technology. Good governance results from sincere high-level management support, buy-in, and cooperation from staff at all levels in the organization. Good governance is transparent, responsive, recognizes and actively engages the organization's greatest security asset: people!

Avoid Sheriff Syndrome—Your Career Depends on It

Security is all about people managing risk. People make poor risk management decisions every day and that can drive your typical security guy or gal absolutely nuts. A key point to remember is that you are not your organization's sheriff. He who owns the risk owns the decision on how the risk will be managed, and how compliance with that decision is to be enforced.

The security department is responsible for designing, implementing, and managing a security program that fairly meets the specific risk-management requirements and other security objectives approved by the organization head(s). The success of any security program depends on support and cooperation from people at all levels of the organization. When things go awry, the vital first step toward finding a solution is to determine whether we are dealing with a **people problem** or **problem people**. There is a very big and salient difference between the two problems, which can be summed up as **can't vs. won't**.

A **people problem** is generally the result of one or more of the following: inadequate training, poorly defined job objectives and performance measures, inadequate supervision/direction, unrealistic staffing levels allocated for task/timeline. **The key message flag of a people problem: "I can't do that."**

When someone tells us **"I can't do that,"** we know we've got a people problem, and the appropriate action is to investigate whether or not the actual true root cause of the failure is with the design, implementation, or operation of the security program itself. Where the program is found to be overly complicated or time consuming, or we haven't provided adequate tools and training to our subjects, the security program manager must work with the actual risk owner and the affected business process owner(s) to determine how to be best resolve the matter.

Problem people ignore or manipulate the approved goals and needs of the organization to suit their own personal agendas. Reasons for this behavior can vary widely from a benign fear of change (i.e., fearing change may lead job reduction or loss) to cloaking far more nefarious insider action against the organization (i.e., activist disruption or industrial espionage). **Key message flag of problem people: "I won't do that."**

If employee attitude (**"I won't do that"**) results in behavior that undermines or interferes with the security program (the organization-approved mission for protecting the organization's assets), then it is up to the organization head(s), the actual risk owner(s), to resolve that problem.

Summing Up

Security controls are used to detect and mitigate risks that are either created or introduced by people. And it is people who are responsible for all the decisions made regarding the design, deployment, and use of security controls. Ergo, people are the root cause of every security control's success or failure—and people are the root cause of every security breach throughout recorded history.

Security governance, programs, policies, and procedures are only effective when the people who must participate in those activities are appropriately informed of their responsibilities, sufficiently trained, and motivated to carry out their security responsibilities. Truly effective security requires building bridges, not just fences.

Darrell Drystek *has over thirty years hands-on experience helping organizations grow positively by providing innovative solutions that focus on the most important part of every business process, information system, and security-assurance program: people. For more of his perspective on why people are your most important security asset, please see the following articles: "Solving the Enigma of Security Awareness" (a seven-part guide for developing an effective training program) and Managing Insider Risk (which discusses issues arising with, and the use of compensating controls for, persons placed in a position of trust). You can learn more about Darrell by visiting his profiles on Peerlyst.com and LinkedIn.com.*

Chapter Seven

Basic Security Hygiene Controls and Mitigations

By Joe Gray

We live in an ever-evolving threat landscape that requires constant analysis and attention. The ideas of old are no longer as universally effective as they once were. Take the information security adage that goes something like, "Red Team attackers only have to be right once, Blue Team defenders must be right every time." I'm not sure that I agree with that—and before you scoff and sigh, hear me out.

That saying was correct before security threats began to exponentially evolve, producing disciplines like digital forensics and incident response (DFIR) and threat hunting. In today's threat economy, we have advanced incident response and zero-day vulnerabilities being exploited both in labs and "the wild," making it nearly impossible for a defender to be absolutely secure all the time. After all, there's this pesky thing called "the business" that we as information security professionals ultimately support, despite what we think or have been told.

What is Security Hygiene?

Security hygiene, sometimes referred to as cyber hygiene, is a new-ish word for what defenders have been doing since network defense became a discipline. According to Wikipedia, security hygiene is "the establishment and maintenance of an individual's online safety." The article goes on to give some examples of security hygiene, including "using a firewall, updating virus definitions, running security scans, selecting and maintaining passwords (and other entry systems), updating software, backing up data, and securing personal data." In short, security hygiene involves taking steps to effectively secure a computer or an entire network from security incidents.

Despite what you see in movies, it's a fallacy that an enterprise defender will always be able to prevent adverse events like breaches and distributed denial-of-service (DDoS) attacks. Instead of trying for the impossible, a better approach is taking the approach Winn Schwartau advocated in his book *Time Based Security*. (You may want to take a look at this YouTube video as well.) Schwartau suggests designing a security architecture based on the time it will take to detect and prevent attacks. While the book is nearly 20 years old, its core idea is still relevant.

Next, we'll discuss examples of hygiene and some implementation scenarios. These are general in nature. Because they're general, they are not intended to replace having an information security professional on staff or making strides to achieve security through corporate policies or compliance frameworks. Note: Compliance does not equal security, but it is a good step in the right direction.

General Hygiene

Defense in Depth

When considering an overall security architecture, comprehension of defense in depth is a prerequisite. There are various layers of defense in depth. Think of it like an onion: Each layer offers a different level (and scope) of protection with different objectives. Figure 1 shows a very basic Defense in Depth model.

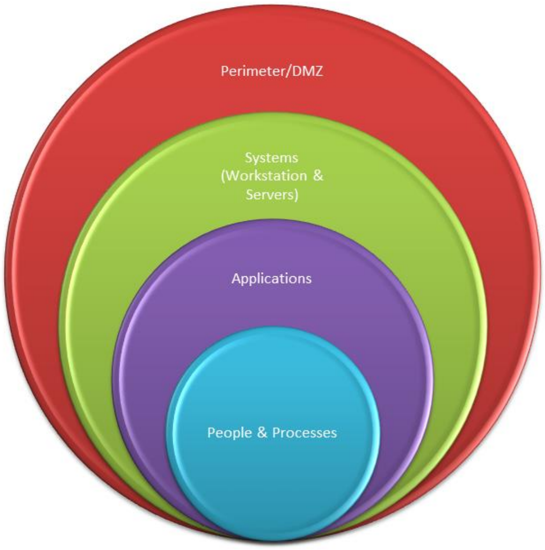

Figure 1 - Defense in Depth

To understand the interoperability of the different aspects of defense in depth, you must realize that each layer performs a different role, yet may also overlap with other layers. Here's a list of the layers and their core objectives:

DMZ (including external Web applications): This is the layer where the company serves the data that enables interaction with outside entities, including the general public and authorized parties. This is sometimes part of an "extranet." These systems can be accessed internally with an internal IP address and externally with a public IP address. Special attention must be paid to the ports and protocols of these systems and access control lists (ACLs) must be employed.

Perimeter: This is the boundary between the DMZ (or outside) and the inside. It's the part of the architecture that controls the flow of traffic in and out of the enterprise. This is where ports, protocols, and services are filtered to ensure that confidentiality and integrity are intact between internal and external zones. Some assurance measures against DDoS attacks are employed.

Network: This is the part of an enterprise that enables the organization to communicate more efficiently and share resources such as an Internet connection, files, printers, and data.

Systems (servers): These are the systems that perform one or more functions to better enable the organization's success. Examples include mail, files, print, application, database, and authentication. They may be Windows, Linux, or UNIX.

Applications (including internal Web applications): These are programs that reside on systems and servers and enable a specific function, such as time keeping, e-commerce, sales tracking, or even security.

Systems (workstations): Workstations are the systems that people use to connect to other resources (network, servers, and the Internet) to perform their duties.

Processes: These are non-technical entities that define how technology is utilized. While they are not specific to defense, gaps in policies and processes can be exploited for attackers' gain, with or without technology.

People: These are the proverbial boots on the ground. They manage the security systems but they also function as HR, accounting, and executives.

Hygiene Strategies and Frameworks

Now that we have defined how defense in depth can be applied to various areas of security hygiene, I would like to introduce three resources that may prove helpful. They are merely starting points, as the act of practicing security hygiene is ongoing and never ending.

Center for Internet Security Critical Security Controls (Formerly known as the SANS Top 20): This document is the primary focus of this chapter. The current version is 6.1. It encompasses various aspects of information security and is a result of collaboration with industry, the SANS Institute, and the Center for Internet Security.

Open Web Application Security Project (OWASP) Top 10: This is a set of controls last published in 2013.

It is pending an update in 2017. This is a starting point for application and Web security. It is a conversation starter for the Application Security Verification Standard (ASVS), also from OWASP.

Cloud Security Alliance (CSA) Treacherous 12 (formerly Notorious 9): This is a list of controls and concerns for cloud security implementations. This is the newest list, but also one of the most vital lists today, as many systems are moving to the cloud in various implementations.

Implementing Basic Hygiene

The Center for Internet Security's first five controls (cited in number 1) above are the basic foundations of cyber hygiene. These controls deal with the inventory of assets and software, hardening systems, vulnerability management, and control of administrative credentials. (The remaining 15 enhance cyber hygiene and are more complex in nature, especially numbers 19 and 20: Incident Response and Management and Penetration Testing.) It is estimated that implementing the first five controls correctly provides security that's as good as, or at or better than, 40 percent of organizations. Implementing the first 18 controls raises this figure to 95 percent.

The first two controls, *Inventory of Authorized and Unauthorized Devices* and *Inventory of Authorized and Unauthorized Software,* deal with whitelisting and blacklisting. These are often referred to as separate methodologies, though they can be combined for additional security. These controls revolve around a simple question: "If you don't know what devices and software exist in your enterprise, how can you properly secure it?"

Whitelisting is compiling a list of authorized devices or software. Blacklisting is naming devices and software that are banned for use within the enterprise. Whitelisting deals with approving all devices and software. This is considered to be more secure than blacklisting. Blacklisting lags in security via the lack of approval of authorized assets.

Next, we deal with having a secure (hardened) configuration baseline. *Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers* integrates with the previous controls by maintaining a formal inventory of installed software and using that as an approved baseline. This can be written or captured as an image. It should be platform (function) and operating system specific and updated periodically, as software versions may change rapidly. From an incident response perspective, this inventory can be a lifesaver when dealing with understanding what event(s) transpired and what modifications were made to systems in an incident.

Continuing through the first five controls, we next encounter the *Continuous Vulnerability Assessment and Remediation* control. This is special, as it allows practitioners to validate the previous controls, and it also help to reduce the attack surface. This control deals with vulnerability scanning, analysis, assessment, and remediation.

Scanning is the act of interrogating systems within specified parameters to ascertain what vulnerabilities exist via checking files, hashes, and versions, among other things. Analysis is the interpretation of actionable output from the scans, and providing it to interested parties. Assessment is an advanced aspect of vulnerability management, one that comes directly before penetration testing. It is the act of applying "what-if" statements to existing vulnerabilities to develop a strategy for remediation. Remediation involves applying fixes to the vulnerability so that it is no longer an issue.

Contrary to somewhat popular belief, not everyone needs administrative privileges on systems. The list of authorized users should be as short as possible, and these users' accounts should be separate from regular user accounts. They should only be used when required so to limit the effect of a compromised user account. This is the essence of the *Controlled Use of Administrative Privileges* control.

Additional Hygiene Steps

The testing of policies, products, and people is a key tenet in implementing security hygiene. Having an awareness program may be an inexpensive way to reduce the impact surface of deficiencies. It also empowers people, by allowing them to understand how their application of security practices plays into the big picture for the whole organization.

Products
People
Processes

Additionally, good hygiene also includes written and clearly defined policies for user consumption. These will drive how products and people integrate. Examples of these policies are:

- Clean Desk
- Password
- Acceptable Use
- Internet Use
- Physical Security

In conclusion, the implementation of security or cyber hygiene is complex and needs much attention. It is always a work in progress, as everything in technology is ever-evolving. I've focused on the Center for Internet Security's first five controls here since they are a solid foundation for security hygiene, including the remaining 15 controls on the center's list. It is my hope that this chapter inspires you to do further research on these controls, or similar frameworks, to enhance the information security posture of your organization.

***Joe Gray** has worked as a systems engineer, information systems auditor, senior UNIX administrator, information systems security officer, director of IT security, and enterprise security consultant. His primary experience is in the information assurance and cybersecurity compliance field. His certifications include CISSP-ISSMP, GCIH, and GSNA. To hear more from Joe, check out his Peerlyst profile.*

Chapter Eight
Understanding Central Areas of Enterprise Defense
By Brad Voris

Enterprise systems require constant monitoring, management, and improvement to protect them and mitigate risk. The central areas where information security personnel should focus to help mitigate risk are: attack surface reduction, application security, network security, endpoint protection, and mobile security. This chapter goes over each of these areas, the risks associated with them, as well as mitigation suggestions.

Attack Surface Reduction

Attack surface reduction sounds daunting, doesn't it? If it is a journey you have yet to undertake…what do you need to consider? You want to mitigate the loss of data, and minimize interruption of communications and processes. Here are the bases you'll want to cover:

- **Encrypt your critical data.** PII/PHI/PCI/SOX or whatever your regulatory requirements are, most require that you encrypt both data at rest and data in motion. Follow industry standards and regulations. Comply with local, state, and national laws. If encrypted data is compromised, the risk is minimal to the enterprise.
- **Focus on perimeter security.** Perimeter security is crucial: not just north and south, but east and west as well. Limit connectivity to and from your systems with firewalls and access-control lists. These will prevent unneeded traffic from the perimeter as well as on the internal network or DMZ.
- **Close unnecessary ports, remove unnecessary software, and patch vulnerable systems.** Unnecessary software will require additional patching and vulnerability management. Use a fresh OS with the latest service packs and patches. Use the latest versions of software with current patches.

- **Change default vendor user names, passwords, and ports wherever possible.** Anyone can get a list of default user names, passwords, and ports online from the manufacturer for troubleshooting an application or system. When default credentials are used in production environments, those applications and systems become vulnerable to compromise.
- **Monitor all systems, processes, and traffic to and from those systems.** Include intrusion detection and prevention systems, or possibly unified threat management, to mitigate the risk of attack. Deploy a security information and event management (SIEM) system to monitor events and correlate data into comprehensive information.

Application Security

- **Establish secure development standards.** Agree on a common coding language, storage, privacy, and management with your development teams. Use auditing and a change-management review to validate that coding is up to secure development standards. Consider utilizing Open Web Application Security Project (OWASP) for developing secure applications.
- **Make the most of the SDLC.** Security, development, and DevOps should be familiar with the software development lifecycle (SDLC) and some of the methodologies related to SDLC. Agile, Spiral, Waterfall, etc., are common frameworks for SDLC. These frameworks help manage the complexities of planning and management of software development from inception to retirement and migration. Through the SDLC and change management processes, fuzz testing should be completed to determine if malformed data or data injection can occur within the code design. It is best practice to look at known vulnerabilities and plan code around them.
- **Develop with encryption in mind.** Encrypt data in transit and at rest with a minimum of AES 256. When possible, use tokenization to minimize the amount of data that can potentially be compromised.

- **Consider federation or single sign-on to centrally manage users, admins, and resources across a domain.** Employ tokenization of user credentials across multiple systems. If a token or system is compromised, either can have authorization compromised.
- **Secure and control application programming interface (API) keys across the domain.** Use best practices when using API keys. Design and use API keys with the minimal amount of access required to complete business functions.

Network Security

The means of transportation and data delivery is probably the most crucial to be protected, as it determines nearly every avenue of attack. After all, if the system is not connected to anything, there can be no outside attack. What is the attack surface of that system? What are the known vulnerabilities of said system? It is really difficult to determine, if there isn't a means of communication to that system.

- **Your ISP can help.** Internet service providers (ISPs) typically have some sort of distributed denial of service (DDoS) prevention system or intrusion prevention system (IPS) system built into their network before it gets to the demarcation point (also known as the de-marc or point of entry from the ISP to the customer's interface). Contact your ISP to see what type of facilities it already has in place to monitor and protect your network from attack, as well to report on inbound/outbound traffic.
- **The router is the ingress point from your ISP into your network, and the egress point for everything outside your network.** Consider following security best practices and set restrictions on your routers. Change the default admin usernames and passwords, keep firmware up to date, force all traffic through your firewall, block access to and from unneeded networks, use banners or messages of the day for anyone that tries to access a device. Some routers are managed by ISPs, which limits the access to the router. In that case, you can request an audit report on the router from your ISP.
- **Intrusion detection systems (IDS) and intrusion prevention systems (IPS) can help mitigate risk of attacks.** These systems can detect potentially malicious traffic on the enterprise network or in the DMZ. Once detected, the malicious traffic can either be

terminated or logged for later reporting. IDS/IPS systems can monitor traffic based on IP address, port, protocol, or even drill down to the application layer.

- **Network segmentation is dividing your network into zones, the most common of which is the demilitarized zone (DMZ).** As discussed in the attack surface reduction section above, you should segment your traffic beyond just north/south firewalls, but also using east/west firewalls. Segregate systems that have access to sensitive data both in the DMZ and in the LAN. DMZs are a type of network segmentation that specifies what traffic from the Internet is allowed access to a segment of the enterprise network. Usually DMZs are made of up firewalls, Web servers, and application servers that need direct access to the Internet to function or allow end users to remotely access those systems.
- **Firewalls are typically the next line of defense after the router.** They help to segment each network and limit access by restricting IP addresses, ports, services, applications, etc. Firewalls should have a limited number of administrators per rule (100 rules to every admin), a minimal number of "any" rules (rules that allow traffic to or from any location), have a review of rules annually, and a change-management process. Most firewalls now have a unified threat management platform built in that includes other capabilities to mitigate against potential attacks. It is always good practice to log all traffic inbound and outbound on firewalls.
- **Email security starts at the firewall level.** Email security gateways help to maximize legitimate mail coming into the enterprise network, and minimize the amount of spam and malicious attacks to the enterprise mail server. Email security gateways act as a layer of defense to filter spam and to mitigate any email attachments potentially containing virus or malware infections.
- **Switches provide the basic backbone of networking but can also help secure a network.** Switches have some basic security functionality such as access control lists (ACL), packet filtering, port monitoring, network admission/access control (NAC), and virtual local area network (VLAN) segmentation. Best practice suggests validating that switches are configured with proper trunk or access port protocols designated for the

right network location and systems to help secure the network. This will minimize VLAN hopping/jumping. Switches also have the ability of network access control (NAC). NACs allow networks to maintain policy requirements that manage access port control. If a client connecting to the port does not meet the specific policy requirements, the port can be shut down or forced to a segmented VLAN to minimize access to the network until the requirements are met.

- **Make the most of proxy servers.** Proxy servers are an intermediary for client requests to servers. They typically pass requests and responses over the Internet from users to servers. There are two types of proxy servers: open proxies and reverse proxies. Open proxies are servers that forward data from a user to a server or multiple servers. Reverse proxies transport client traffic to a destined server, but responses appear as if they are coming from the destined server, not the reverse proxy server. Usually, proxies are used for end users to communicate with servers on a private network.
- **SIEM isn't just a four-letter word.** Security incident emergency management (SIEM) is a tool designed to aggregate and correlate security event data from systems to provide reporting. Most SIEM products have extensive built-in features like compliance reporting, dashboards, real-time alerts, and forensic analysis. Although SIEMs are a great tool, they require specialized training and are very expensive. Size a SIEM based on the enterprise's business needs, expected growth, and existing infrastructure environment.

Endpoint Security

Endpoint security measures are crucial to mitigating against risks in your enterprise environment and play a key role in defining the enterprise's security posture. Providing a solid security foundation for endpoints will ease the burden of administration.

- **Endpoint privileged access is absolutely crucial.** One of the biggest constraints for endpoint security is end user administrative requirements at the endpoint level. End users may have specific business requirements for admin rights—however, not all end users require admin privileges. Limiting admin rights to end users on endpoints will improve security. A standard endpoint user should not install software, add hardware, or make system changes without contacting the help desk or IT support. Forcing the end user to seek approval from one of those governing entities could ultimately prevent spyware, rootkits, virus infections, etc.

- **Make use of two-factor or multifactor authentication protocols where applicable.** Two-factor and multi-factor authentication protocols are great addendums to an existing enterprise security posture, and a requirement for some regulatory compliance. Two-factor or multi-factor authentication relies on the basic principle of "what you know, what you have, and what you are." This means that at least two or more of these items are required to access a system:
    - What you know: PIN, password, passphrase, etc.
    - What you have: HID card, badge, token, etc.
    - What you are: Biometric access (fingerprint, retina scan, voice/facial recognition, etc.)

  If two or more of these factors are required for authentication, it makes it incredibly difficult for someone other than the end user to authenticate to the endpoint. The first two factors are relatively more cost-effective to implement than the later. Although it's the most accurate, biometric authentication is the most expensive. Choose the right fit for your organization based on the sensitivity of data and the compliance requirements in your industry.
- **Endpoints are dynamic and need to be protected with tools that are flexible, like a centralized threat management platform.** Endpoints may move from the enterprise network to a public network, potentially exposing themselves to risks associated with a lack of security controls on that network. A centralized threat-management platform that has antivirus, anti-malware, application sandbox, and firewall capabilities at the endpoint level is critical to protecting, updating, and enforcing policy on these endpoints. Choose a good fit for the organization, and a platform-agnostic approach that protects all endpoints. Then monitor to validate that updates have been pushed

through to the endpoints. Endpoint security tools should have minimal end user impact; and automatically update, detect, alert, and remediate any security-related issues.

- **Consistent updates and patch-management systems that mitigate against vulnerabilities should be implemented**. These systems should be in line with your environmental requirements and log updates (what was updated, when it was deployed, and who deployed it). Having this information integrated with the change-management system will help mitigate issues related to patches that fail or cause issues with applications or system configurations.
- **Keep data where it belongs.** Endpoints (laptops, desktops, mobile devices) should not store sensitive business-related data. In order to prevent storage on endpoints, policies (business policy and software-defined policy) should be in place to keep end user data in the enterprise. A virtual private network (VPN) solution should be provided to mobile endpoints, giving end users access to the resources that they need. Endpoints should have built-in encryption software.
- **Standardization will greatly improve endpoint security.** Consistent software and hardware platforms will mean consistent patches and known vulnerabilities within the enterprise. Knowing these vulnerabilities, and ways to mitigate them, will improve overall security. Steps to centrally manage hardware and software platforms will be considerably easier within the organization. However, standardization is not without its pitfalls. If there are vulnerabilities in systems that manufacturers have not addressed or have no timeline to address, it leaves those systems at risk.

Mobile Security

Mobile device security… it sounds almost cringeworthy. How do you secure something that rarely touches your network directly? How do you manage, update, and enforce policy on a mobile device? It isn’t as challenging as it was in the past. With the advance of mobile devices, came the advance of mobile device management (MDM) systems.

- **Mobile Device Management Systems.** MDM systems are available from nearly every major manufacturer. Most allow for fairly granular policy deployment and enforcement, which greatly improve mobile security. These systems can prevent installation of third-party applications that are not approved by the organization, protect mobile devices with antivirus and anti-malware software, and provide a secure connection via VPN tunnel back to the organization. Most MDM systems also have remote wipe capabilities in the event of loss or theft. Selecting the right MDM solution for your organization may be difficult, due to the multitude of platforms across your organization. So look for an MDM system that's platform agnostic. It must protect and cover the standard devices in the network, as well as bring your own devices (BYODs).

***Brad Voris** is an information security manager at Vroom, Inc. He specializes in infrastructure architecture and security design, and has designed and managed infrastructures for global organizations. He holds CISSP, MCP, MTA, NSE1, Network+, and VCA-DCV certifications. To hear more from Brad, check out his website www.VictimOfTechnology.com or his Peerlyst page.*

Chapter Nine

Telecom Security 101: What You Need to Know

By Eric Klein

What Is Telecom Fraud?

In very general terms, telecom fraud is fraud using a telephone or telephone system. Let’s start with what this chapter is not covering before explain what is included.

I will not be covering the multitude of malware on smartphones or the various types of fraud that use a telephone to trick people out of money (“this is agent xyz of the IRS calling…”) or to phish call centers.

Here I will address the attacks on a company telephone switch—a public branch exchange (PBX)—that is on premises or hosted. Unlike other attacks, these are designed to directly take cash out of your company’s bottom line. Although it should be noted that these kinds of attacks are starting to be possible via home switches that are available for as little as $20 or potentially your smartphone, this type of fraud is the same regardless of target. It is just that companies frequently have the capacity for more concurrent calls—increasing the “take” in a shorter time.

How Big Is the Problem?

Telecom attacks are on the rise because of some very basic considerations. This kind of crime is relatively low risk, the online tools and software that can target these services have proliferated, and there are more targets than ever before as PBXs have become more affordable.

Over the past several years, the average attack on a company results in $25,000 to $50,000 (in U.S. dollars) in losses over about 48 hours. In almost all cases, the customer is responsible to pay for this fraud. In one particularly bad case, a company lost $400,000 in 48 hours. On the other hand, there are some hopeful examples, including a case where the company used best practices and was able to refute $300,000 worth of fraud.

By comparison, SQL servers—which represent the second-most attacked category—account for only 4 percent of attacks.

The Communications Fraud Control Association (CFCA), whose members include law enforcement as well as major and minor telecom carriers, works to monitor and fight these kinds of fraud. Every two years, they survey their members about the levels of fraud they are seeing. According to the CFCA 2015 Global Fraud Loss survey, the estimated total cost of telecom fraud is $38.1 billion annually. The survey also found that 89 percent of operators said fraud losses had increased or stayed the same as the previous year.

Top Fraud Methods

According to the CFCA 2015 Global Fraud Loss survey, the two largest losses came from:

1. $3.93 B – PBX Hacking
2. $3.53 B – IP PBX Hacking

   Making the total loss from hacking PBXs $7.46 billion dollars. In almost all cases, this is money taken directly from customer switches that the phone companies require them to pay. Let’s look at who is attacking and how these charges are accrued.

Who Is Attacking?

There are many different types of attackers looking for your system, these include:

- Organized crime—PBX hacking is a low-risk, high-return crime
- Terrorists—who use the funds to fund more terror
- Hackers for hire—working for either of the above groups
- Kids for fun (and bragging rights)

In the past, criminal and terrorist groups had better ways to fund their activities, but now telecom services make up a significant part of their income. Sometimes these are direct attacks, and other times they are outsourced. For example, in 2013 Al Qaeda outsourced the hacking of AT&T customers for over $2 million, paying the hacker only $4,000 for that service. One dry-cleaning company in New York was hit with a $150,000 phone bill for nearly 9,000 overseas calls.

What Do They Get from Hacking your PBX?

Successful attackers gain access to telephone lines from which they can make calls to foreign countries and premium-rate phone services. Long-distance services can be sold on to phone shops, while attackers can make up to $1 a minute by calling premium-rate numbers that they control.

Here's where some of that easy cash comes from:

- Free phone calls at your company's expense (this can include internal fraud, where employees make unauthorized international or premium calls).
- Non-employee, but still internal (cleaning, delivery, etc.) staff making calls that are not properly authorized.
- Reselling phone services—using your phone service to make calls while charging someone else or them.
- Cash from premium calls (1-900) where the hacker shares in the revenue from a local phone company. Rates can range from $1 per minute to as much $19 per call.

- In very rare cases, PBX hacking is just done for bragging rights (but that is mostly history now). For example, people like Steve Jobs and Steve Wozniak built Blue Boxes to make illegal free long distance calls, just to prove that they could do it.

As you can see, there are many ways hackers can make money off of your company's PBX, and as these can be multi-country attacks, they are hard to prosecute. For instance, in the example cited in the previous section, Al Qaeda groups in the Philippines and Somalia hired Italian hackers to target American companies by making calls to an international premium-rate number.

How They Find and Attack You

Finding Your PBX

As with any connected device, there are ways to find and identify your PBX and even your voice-over IP (VoIP) phone. The most common way is for someone to do a scan of the full IP address range. There have been several such scans published, and there is even a site that does it regularly, updating details like IP address, protocols responded to, type of hardware, operating system, and even if the device is using the default password. In fact I have run a VoIP security training class where we demonstrated one of these, and within one minute of showing the list of VoIP phones from one manufacturer, someone had accessed the first one listed using the default user and password.

Attack Types

Like other IP-connected devices, phones and PBXs are hit with similar attack types. Some examples are:

- **Brute force.** Used to try and crack the security for access usually using a customized dictionary of common user names and passwords.
- **Denial of Service (DoS).** Used to block service, usually to prevent authentication calls from banks and credit card companies, but also just to block service to a number or PBX.
- **Spoofing.** Pretending to be a customer to the carrier, or pretending to be an authorized connection to a company's system in order to make calls at its expense.

How to Protect Your Company

Now that we have established who is attacking, how, and why; let’s look at what you can do to mitigate these attacks.

Address Common Policy Problems

Do you need to allow all calls all the time?

Are there hours when your PBX should not be in use, other for emergency services? If you are closed weekends or holidays, then you should not have calls permitted during these times. See what options your system or carrier offers.

Who needs to call international or premium-rate numbers?

In most companies, there are very few, if any, individuals who need to make international or premium-rate calls. In fact premium-rate calls should be so rare that they should be authorized on a per-case basis. See what options your system or carrier offers.

Which phones need voicemail?

It is quite common to automatically assign a voicemail to every extension, but this is not wise. Voicemails can be configured to forward calls to the outside. So do you need a voicemail for the phone in the lobby (and does it need international access?), or even the server room? Consider where voicemail is likely to be needed or used, and where it is just there as an automatic addition.

How do you handle an employee leaving?

Frequently, phone extensions are left active even after an employee has left. Again, this leaves a voicemail as a weak link for attacks. Better to either delete or deactivate the extension until it is needed again.

Fix Common Configuration Problems

Default passwords

As a general rule, you should change default user names and passwords for all systems, not just PBXs and phones.

Servers (PBXs)

Change from default user name and password, and if possible, change the server name so it doesn't indicate to outsiders that it's a phone switch. If your provider allows it, switch from using the standard port (5060) to a different port.

Phones

Change from default user names and passwords, and, if your PBX and phone both allow it, change from using the standard port (5060) to a different port.

Voicemail

As stated above, after determining which phones should have voicemail accounts, make sure that they do not use the common passwords (0000, 1111, or extension number). This should also be the case for cellular voicemail systems.

Block Common Fraud Destinations

Beyond the decision about where the company needs to make legitimate calls, there is the need to block calls to places you don't do business, as well as the most common fraudulent-call destinations. These are usually places with high payouts for premium numbers, or countries that lack oversight. According to the CFCA 2015 survey, the top five countries where fraudulent calls terminate are:

1. Cuba
2. Somalia
3. Bosnia and Herzegovina
4. Estonia
5. Latvia

So the obvious question is: Does your business have any legitimate reason to call any of these countries? In most cases, the answer is no. See if your PBX, monitoring system, or carrier has the ability to block calls to unnecessary international and premium-rate destinations.

Block Off-Hour Calls

Many cases of telecom fraud happen during hours when a company is normally closed. This is mostly because they are less likely to be noticed and more lines are available for concurrent calls. If you are not running a 24x7 business, it is best to have outbound calls blocked when the company is closed. You should allow night staff to make local or other appropriate authorized calls, and block everyone else. Check the settings on your PBX and with your carrier to configure these restrictions.

Remove Unneeded Voicemail Accounts

As pointed out above, you need to look at which extensions should have voicemail, and when to close voicemail for employees who have left. It is easy enough to disable voicemail and then re-enable extensions when warranted.

Proactive actions

Understand your Contract

Read your contract to find out various conditions or available functions, but make sure that you get everything in writing in case you need to challenge it later.

- What is your liability for fraud? This will vary between carriers and will have different levels of “required prevention effort,” so know what you’re paying for.
- Know the procedures for identifying and reporting fraud.
- Know what options you have to monitor phone charges during the month, rather than just when a bill is issued. Some carriers only provide detailed reporting upon request. Make sure that you always get bills detailed by call, as well as extension, if possible. This will enable you to compare what your PBX sees and what the carrier sees.

Set Rules with your Phone Company

See what options you have for destination and time of day/day of week limitations on the calls. If you activate these and fraud happens, it is the carrier's responsibility, not yours.

Monitor Activity

Have proactive monitoring so you can know what's happening during the month and not only two to six weeks after the fact. Keep call detail records (CDR) files for at least six months; and for some businesses, you may need to keep them for up to seven years. These can be priceless when challenging your carrier on fraudulent charges (see the $300k example earlier in this chapter). Use monitoring and business-intelligence tools to look for abnormal peaks in traffic, or calls to strange destinations.

Use a SIP-Aware Firewall

Put your phones behind a session-initiation protocol (SIP) aware firewall. This will allow you to set VPNs, secure access, and limit the chances of people finding your devices. There are even several single-line SIP firewalls available for under $100 each that can be used for remote sites that don't have their own full firewall, such as home offices. Try to do everything in point-to-point or back-to-back IP virtual private networks (VPNs) that will prevent others from connecting. These are useful for either regular VoIP desk phones, as well as softphones that run as a program on your computer or mobile device.

Conclusions

Although the attacks are becoming more common, a little common sense can protect your company. Most exploits take advantage of lax policies (especially passwords) that can easily be fixed. An hour of configuration changes can protect your company from extensive liability and costs.

***Eric Klein** has more than 22 years of experience in the telecom industry. In addition to his experience in VoIP security as vice president of operations at his current company, Greenfield Technologies, Ltd., he did fraud prevention at Humbug Telecom. He has also worked for carriers MCI Communications (now part of Verizon) and Cellcom. Eric co-authored "RFC4864: Local*

Network Protection for IPv6," served as a grant reviewer for the U.S. Department of Commerce Broadband Initiatives Program (BIP), and the Broadband Technology Opportunities Program (BTOP). He publishes "Term Tuesday" blog posts at least twice a month on Peerlyst and is the Peerlyst Ambassador for Tel Aviv. You can find his Peerlyst profile here.

Chapter Ten

Strengthen Your Security Arsenal by Fine-Tuning Enterprise Tools

By Puneet Mehta

The growing shift towards digital transformation is causing a major challenge for businesses in terms of complexity of security requirements due to changing hacker tactics, increasing security vulnerabilities, extended enterprises, and emerging security technologies. Every now and then there is a surprise disclosure of a massive new data breach, and it's time for a reality check: This is a sign that organizations are losing the security battle, especially against new age targeted cyberattacks.

The motives behind data breaches are diverse, but often the hackers looking for some easy financial gain go after the low-hanging fruit—the vulnerable, unpatched, and less-secure systems in the enterprise—to achieve their motives. The biggest lesson we need to learn from these breaches is that today's advanced threats require a far more proactive and concrete strategy. Security teams cannot operate in reactive mode, responding to alerts of potential threats. Today, hackers with malicious motive can penetrate traditional defenses, compromising any critical infrastructure within minutes or hours. By the time your company learns and uncovers an intruder (which might take weeks or months), your confidential data or digital assets are likely to be already compromised. When even organizations with huge security budgets and resources experience massive data breaches, it signals that a major shift is needed in the approach to defending against advanced threats.

Smart organizations should therefore be continuously reassessing their security arsenal and fine-tuning it to get the most of their security investment. Whether commercial or open source, all security tools require calibration and adjustment, which helps security teams to closely control how the tools should behave, interact, and respond to any security incident. Unlike waiting for potential threats to be surfaced by an alert, well-configured, integrated, and fine-tuned security tools let your security team be proactive in identifying threats sooner. This tweaking or fine-tuning should not be an ad hoc activity. Rather, it should be a critical component of the strategy for protecting your company’s digital assets and confidential information.

The other thing that needs to be considered is that it’s not always the tool that requires fine-tuning, sometimes it’s the initiative or program that must be re-aligned to meet organizational security objectives. There is a greater need to formalize security programs, security architecture, and underlying processes to deal with threat defense. As is quite common, your security team may not call it a formal cybersecurity program yet, but chances are good that they are searching for threats already. For instance, your team may be analyzing and correlating logs and using forensics on data sets, or matching threat-intelligence feeds with data. Now, while their activities may not be formalized, and might not use all the right data or tools, they are already moving in the right direction.

To be effective, every security program and tool must be implemented, configured, and tuned to match your business logic and identify the risks that matter most to you. Without these steps, the high cost of adoption will outweigh the potential benefits of your investment. Security teams must sharpen and deploy their tools to match the business requirements, technology environment, integration level, and security policies of their enterprises. Pro-actively accounting for these attributes will:

- Improve the accuracy and effectiveness of tools
- Reduce the noisy false positives
- Minimize the costs and resource drain that could be arising from deploying inefficient, ineffective security measures
- Make the most of the enterprise security architecture
- Provide a greater level of integration among security tools to enable wider coverage and visibility

If you’re someone who is responsible for managing enterprise security, read on to understand why fine-tuning your security tools is imperative today—and how you can make your investments in security tools as effective as possible to stop advanced threats and prevent serious damage to your company.

Here are the top 5 reasons you should be fine-tuning your security tools:

1) There’s too much noise.

Thanks to technologies such as UTM, SIEM, advanced threat protection, and other emerging sources of security information, security teams are now able to capture more critical data about threats and attacks. By being knowledgeable on the latest threats, security teams are better equipped to help strengthen the security posture of organizations in a big way. While these tools provide you with unprecedented information, they can also lead to the generation of false positives, which is a normal or expected behavior that is identified as anomalous or malicious. False positives are a problem not only because they take up a lot of effort and time, but also because they can lead to distraction in dealing with legitimate security alerts. Further, the impact of false positives increases as you add more layers of security defenses.

A good example of how false positives can have an impact is the Target data breach, where the technology used to monitor intrusions provided multiple alerts on different occasions regarding suspicious activities. But since those alerts were buried in hundreds of false positives, they became deprioritized on the list of security items, resulting in a major data breach.

In order to make sound decisions around enterprise security, it is imperative to have good information. So it becomes important for the security teams to spend as much time as possible in capturing and documenting their security monitoring and alerting needs. You’ll need focus, patience, and time to adjust your tools (SIEM systems, log analyzers, intrusion-prevention systems, security scanners, anti-malware tools, among others) to ensure you're getting the most out of them. You’re still going to get false positives, but you can reduce them over time.

It is really not uncommon to see these issues in tools that are not properly operationalized, such as when tools are installed and deployed using default settings and profiles. To address this issue, your teams require a great deal of fine balance. The best way is to start with a thorough understanding of what a given tool is intended to address, as well as its expected behavior. It is imperative to ensure that the implementers fully understand the intent of the tool deployment, rather than making assumptions about the common use cases, or simply installing a tool with default settings.

When configuring and tuning new security tools, security teams need to take an incremental and phased approach complimented with a thorough understanding of the environment they are protecting to make intelligent tuning decisions. Tuning is an ongoing process that needs to account for changes in the environment. There needs to be a thorough process to test the updates and capture the changes they bring in, so that those specific alerts can be filtered and/or dismissed, leaving a clear set of actionable alerts for administrators to follow up on.

As a reality check, any security tool implementation will impact existing policies and procedures, including your incident response and other operational procedures for systems that the tool impacts. This impact should be thoroughly reviewed and validated, and policy and procedures updated accordingly in order to ensure that operational activities are minimally impacted by the change.

2) You want to learn from incidents

Advanced persistent threats (APTs) are definitely the most devastating type of incident. As a common behavior, an APT may stay invisible for a long time before finally causing serious financial damage and harming a company's reputation.

Mandiant's annual cyber threat report *M-Trends 2016* stated that "the average number of days organizations were compromised before they discovered the breach (or were notified about the breach) in 2015 was 146." Just imagine the damage caused over those five months. The discovery of APTs is limited to the power of the monitoring controls you have in place.

Even as the list of attacks gets longer, it's clear that some of these breaches could have been prevented if basic security hygiene was maintained. Many breaches can be attributed to weak configurations, loose integrations, and default security controls, ad hoc authentication schemes, and increasing false positives alarms. All of this makes it evident that fine-tuning security tools is an essential—and ongoing—process.

3) To address the limitations of traditional siloed tools

With the increase in breaches, it's common to assume that organizations might not be taking adequate security measures. But in reality, the victims usually had adopted the whole range of security tools, from standard firewalls and anti-virus programs to anti-malware products and more. Managing a wide range of security tools is difficult and costly, as it demands investment in both licenses and resources. Additionally, manually correlating data from multiple systems in order to detect and respond to proliferating attacks becomes increasingly impossible. And finally, scattered solutions and siloed approaches cannot ensure complete coverage of a company's IT environment, which may result in loopholes that let hackers in.

The problem with traditional tools is that they are often deployed in silos and lack integration capabilities. This limitation leads to a big security gap that makes the tools unable to withstand new type of attacks—and that leaves a great number of blind spots in an enterprise's infrastructure. To overcome this gap, look at integration capabilities coupled with automation to achieve the best results from your existing security investments.

4) You need to manage the increasing complexity of digital transformation

Extended enterprise is the reality of today and can't be ignored. The increasing mobile, cloud, and connected device adoption trends are opening new opportunities for attackers—and that's making it more difficult for defenders to secure their digital infrastructure. Research from the Enterprise Strategy Group shows that "79 percent of security professionals believe that network security has become more difficult and a virtually equal percentage (80 percent) believes that traditional security management and operations are more difficult as well." The reality is that traditional security tools such as firewalls, IPSs, security gateways, data-loss prevention systems, and other countermeasures were mostly designed as on-premise solutions for networks that are physically bound to specific locations. Now, when your endpoints have no boundaries, it's becoming challenging to make sense of all the data being collected and spot anomalous activity using traditional defense systems.

Organizations should now reevaluate their defense mechanisms and re-examine their security investments in order to stay protected from new-generation attacks. This also requires fine-tuning and integrating targeted solutions to offer more visibility and controls, as well as possibly investing in newer security tools to bridge the critical gap against new threats and attacks.

5) To keep up with shifts in the attack surface

As the threat landscape changes, the attack surface is becoming hard to defend. Adversaries are using advanced techniques to pass through perimeter defenses, ignoring detection technologies. It's possible for attackers to be in your environment and stay as long as they want to compromise critical infrastructure and cause severe damage.

Traditional security solutions lack advanced features and may focus on one or two steps in the attack chain, but tweaking, integrating, and automating them to effectively participate in the defense system may prove to be helpful. The data sets that can be automated and integrated might include operating system events, Network data, application logs, and other relevant data collected by your security systems. By analyzing the data and following the digital footprints of the attacker, security teams can be in a better position to at least defend against known attacks. It may also be a wise decision to invest in advanced security tools if it’s determined that existing tools fail or lack capabilities in critical areas.

Summary and Recommendations

Here are some recommendations and best practices that security pros can implement to get the most from their security arsenal:

- The more logging you do, the more tuning is involved. There will be a high false positive rate if you don't do fine-tuning. Basically, that involves getting a thorough understanding of the security tool interface and making changes to out-of-the box rules so that the tool is making the most accurate assessment it can.
- Despite their many benefits, advanced security tools such as SIEMs are only as useful as the information you put into them. If you feed them with un-validated, raw threat data, then the outcome is not pretty. Today’s advanced security tools hold a well-deserved place in your security arsenal to hunt advanced threats, but to truly shine, they need to be fine-tuned and sharpened to produce the meaningful information that security teams can rely on confidently.
- To bridge operational and data silos across risk and compliance functions, an effective strategy requires fine-tuning the existing security architecture. This approach enables intelligent security operations that can support the current status quo, but are still able to evolve and embrace new technologies while mitigating new risks and supporting new compliance requirements. Re-aligning the security architecture to meet new

requirements encourages a balance of preventative, detective, corrective, and predictive investments.

- Transform your SOC into an adaptive cybersecurity platform. If your enterprise is like most, you have a significant investment in security solutions. The good news is that an adaptive cybersecurity platform actually complements your existing investments while letting you maximize the value of those systems by feeding the intelligence you derive into a system that creates an effective and persistent defense. To gain the most value from your security tools, orchestrate and automate them. Orchestration gives you the capability to connect your siloed security tools into a single glass window, ensuring that they're all working in tandem and cohesively. Then, automation can help streamline the workflows between multiple systems and help eliminate manual, tedious tasks. By optimizing your SOC with orchestration and automation capability, you are not only streamlining the crucial tasks of alert detection, investigation, data enrichment, and response, but also minimizing the alert fatigue. This will help your security team respond to incidents faster and more effectively.

***Puneet Mehta** is a security researcher, author, speaker, and cybersecurity evangelist. He is also the former co-chair of OWASP India and former director of the ISACA Delhi Chapter. He has authored many articles, blogs, and whitepapers, as well as been quoted in national and international media. Puneet is a frequent speaker and contributor to various cybersecurity research consortiums and industry forums. His focus areas include threat intelligence, investigative research on advanced cyberattacks, and APT; and his certifications include CISSP, CSSLP, CISA, CEH, and CPTS. To hear more from Puneet, check out his Peerlyst profile.*