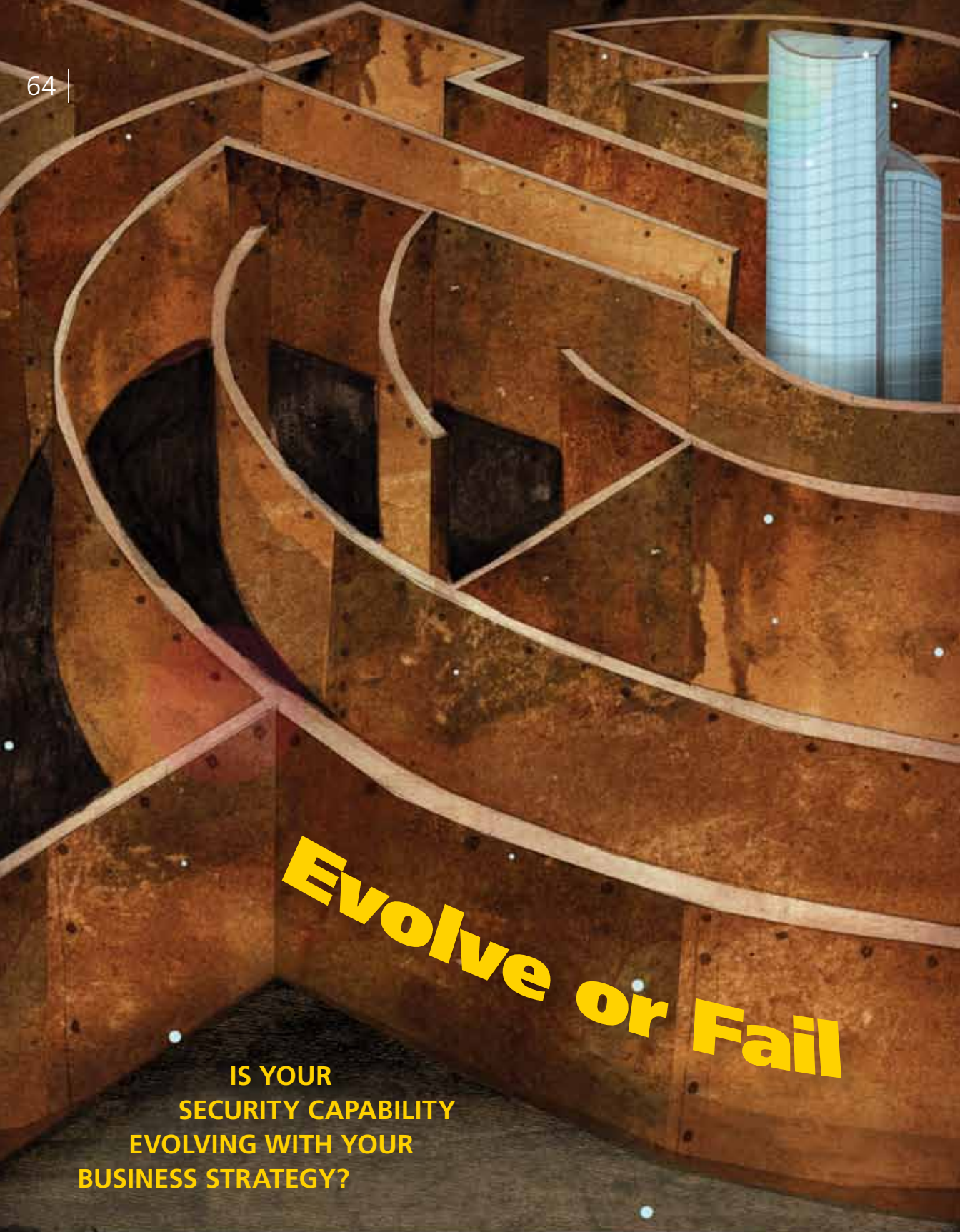


Evolve or Fail

IS YOUR SECURITY CAPABILITY EVOLVING WITH YOUR BUSINESS STRATEGY?

BY TED DEZABALA, IRFAN SAIF AND GEORGE WESTERMAN
> ILLUSTRATION BY MARCO WAGNER

FOR ALL THE TALK IN BUSINESS TODAY ABOUT WHERE THE BUCK REALLY STOPS, A SURPRISINGLY LARGE NUMBER OF SENIOR EXECUTIVES HAVE LITTLE APPRECIATION FOR HOW DEEPLY EXPOSED THEIR ORGANIZATIONS MAY BE TO SECURITY THREATS AND RISKS, SOMETIMES, UNTIL IT IS TOO LATE.

Any experienced leader knows that little is accomplished by those who try to get things done. That's because good leaders don't confuse effort with results. Yet when it comes to security risks associated with technology, where a critical breach can bring a business to its knees, there's a great deal of *trying* going on. And not nearly enough *doing*.

Not surprisingly, many executives today believe their organizations are well-protected. With broad policies in place for technology governance, risk and compliance, most have assigned responsibility for security to their IT shops, confident that their fiduciary and legal obligations are being met. But a closer look at the real risks and threats reveals a different picture. Organizations that take a compliance-oriented approach to enterprise and IT risk may not be managing many of the threats that matter most.

It's not uncommon for companies to equate compliance and security. That's what happened recently when a major retailer was hacked, exposing several million debit and credit card numbers to the risk of theft. The company appeared to have a rock-solid compliance program in place, asserting that they followed all the security requirements mandated by the credit card brands and others. But that wasn't enough. A number of back-end systems were left unpatched, leaving some of their software vulnerable to exploitation. Hackers were able to penetrate the company's systems despite their most diligent compliance efforts. Thousands of cases of fraud were linked to the breach, exposing the company to legal, reputational and financial risks. A risk-based approach using a layered defense could have helped prevent such an incident.

In another recent incident, millions of email addresses were hacked from one of the world's largest email marketing companies. With those addresses in hand, cyber criminals can pose as legitimate companies, threatening to steal even more information through endless phishing schemes and other potential attacks. One leading magazine publisher paid more than $8 million to a scammer pretending to be a legitimate vendor. The perpetrator had posed as the publisher's printer and asked accounts payable to switch the mailing address for their payment check.

But security risks aren't limited to the retail and service sectors, where major breaches make for juicy headlines. Smaller failures and incidents are commonplace in almost every industry, even though they don't always garner immediate attention. In fact, that's part of the problem.

It is often not thought of as a big deal when an employee's smartphone turns up missing. Security teams usually don't get fired when a virus scrubbed from one machine shows up on a different machine a month later. Almost nobody is ever reprimanded for using public Wi-Fi to conduct sensitive company business without the appropriate protections in place on their end-user devices.

In many cases, companies escape the consequences of these low-level threats, but it's not because of good risk management. It's because they're *lucky*. All too often, incidents occur without any knowledge on the part of those who are supposed to detect them, causing many security executives to think of a *quiet* day as a *good* day. Lulled into a false sense of security, they become complacent, creating an environment where small failures can cascade unnoticed into larger, more substantial problems.

With so many people seemingly focused on security today, how is it that security incidents and data breaches still happen so frequently – and then manage to go undetected, sometimes for many months? Doesn't solid compliance ensure that important threats are covered? Don't security teams have everything they need to stay ahead of new threats? Too often, the answers are no and no. Organizations that are perfectly compliant still get hacked.

WHY SECURITY BELONGS ON THE C-SUITE AGENDA

In today's complex operating environments, vulnerabilities are getting harder to manage, even as the threat level continues to increase. To understand the challenge, it's helpful to visualize three evolving environments as the source of elevated risk.

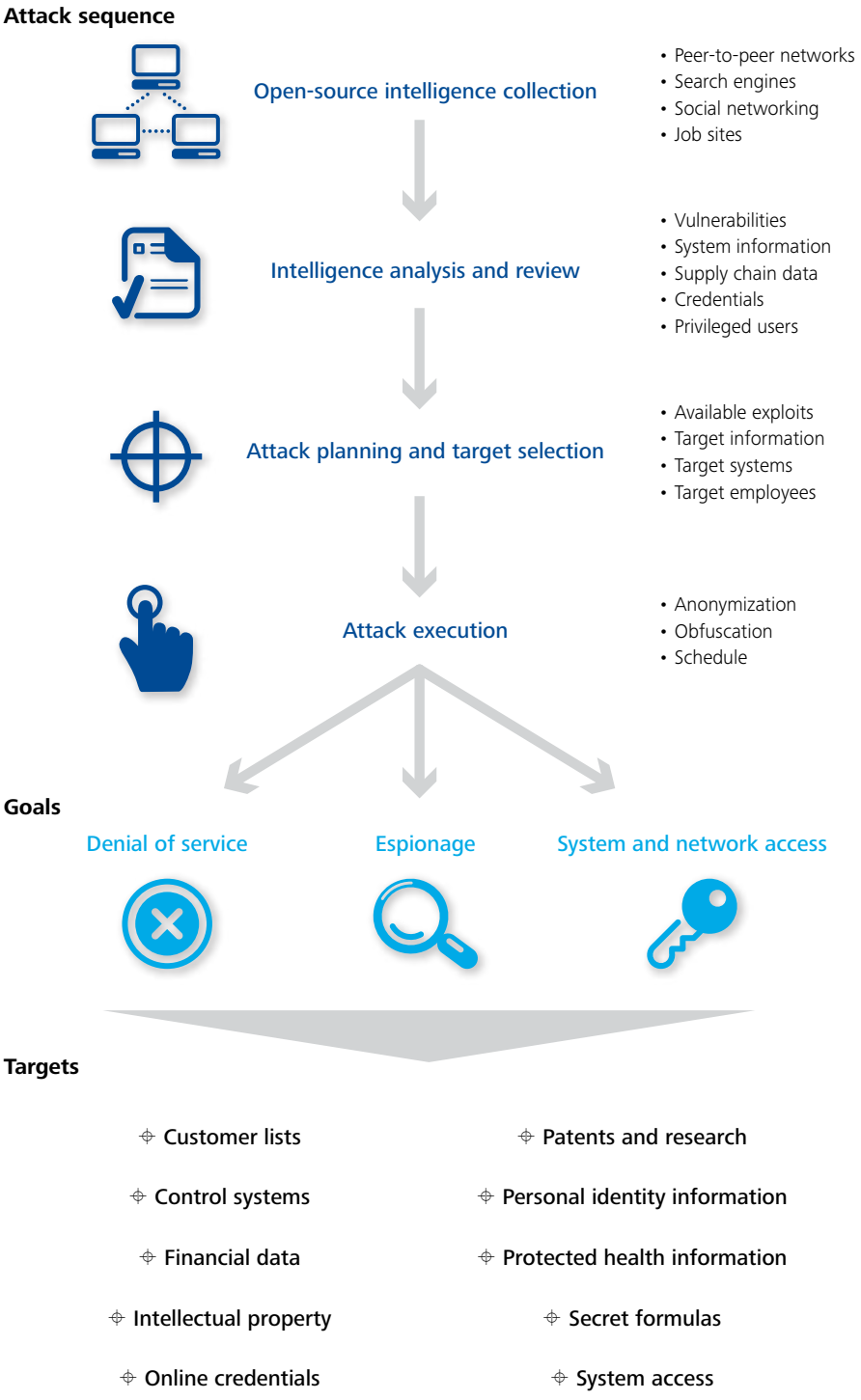
- The ***business environment*** evolves as competitive conditions and customer needs evolve, giving rise to new business models, new processes and new ways of working.
- The ***IT environment*** evolves to support these new models, as well as the changing expectations of users who adopt new tools to stay connected and productive. Often, security professionals are not involved, thus creating new vulnerabilities.
- The ***threat environment*** evolves as changing business and IT environments create new exposures, vulnerabilities and avenues of attack and adversaries become more creative and collaborative in uncovering these avenues of exploitation.

At the center of this storm is the notion of APTs—Advanced Persistent Threats—automated versions of espionage that once relied on human beings operating in the physical world. Espionage has gone cyber, with operatives stealing proprietary information around the clock and around the globe. Unlike physical threats, APTs may not even be noticeable. They can blend into corporate and personal systems, establishing virtual back doors and tunnels, returning to steal again

and again, completely undetected or, increasingly, programming your system to send them information on demand by automating data exfiltration.

Figure 1: Anatomy of a cyber-attack

Cyber-adversaries collect open-source intelligence in order to generate schemes and methodologies for carrying out well-planned attacks in order to achieve their goals.



To navigate the blurring boundaries and proactively manage APTs as a true business risk, organizations need the kind of broad visibility and permissions that reside only with executive leadership. Effective choices require trade-offs that only executives can make. Simply put, if enterprise security isn't on the C-suite agenda, it's not on the agenda that counts. This doesn't mean executives need to be security experts. But it does mean that security considerations must be part of an organization's strategic conversations.

Just consider the relative value of corporate data, systems and intellectual property – and the seriousness that APTs, malicious actors and even employees can pose to those assets. The recent fallout over recent disclosures published by WikiLeaks is one example of trusted insiders uploading confidential information to a public website. When financial institutions and Internet service providers, under pressure from authorities, cut off services to the controversial Web site, their actions triggered sustained attacks from a worldwide army of hacktivists. Operation Aurora is another instance where cyber-terrorists gained access to source code repositories and other intellectual property at nearly 200 global security and defense companies.

Are there circumstances under which your company could be similarly threatened? Are you prepared, for example, to deal with the consequences of a significant breach of private data, either from you or one of your trusted business partners? Do you have a clear game plan to quickly fund and deploy resources when a new vulnerability is exposed? Who in your organization understands which risks matter most – and what you should be doing about them? Do you know what the potential security risks are to your business?

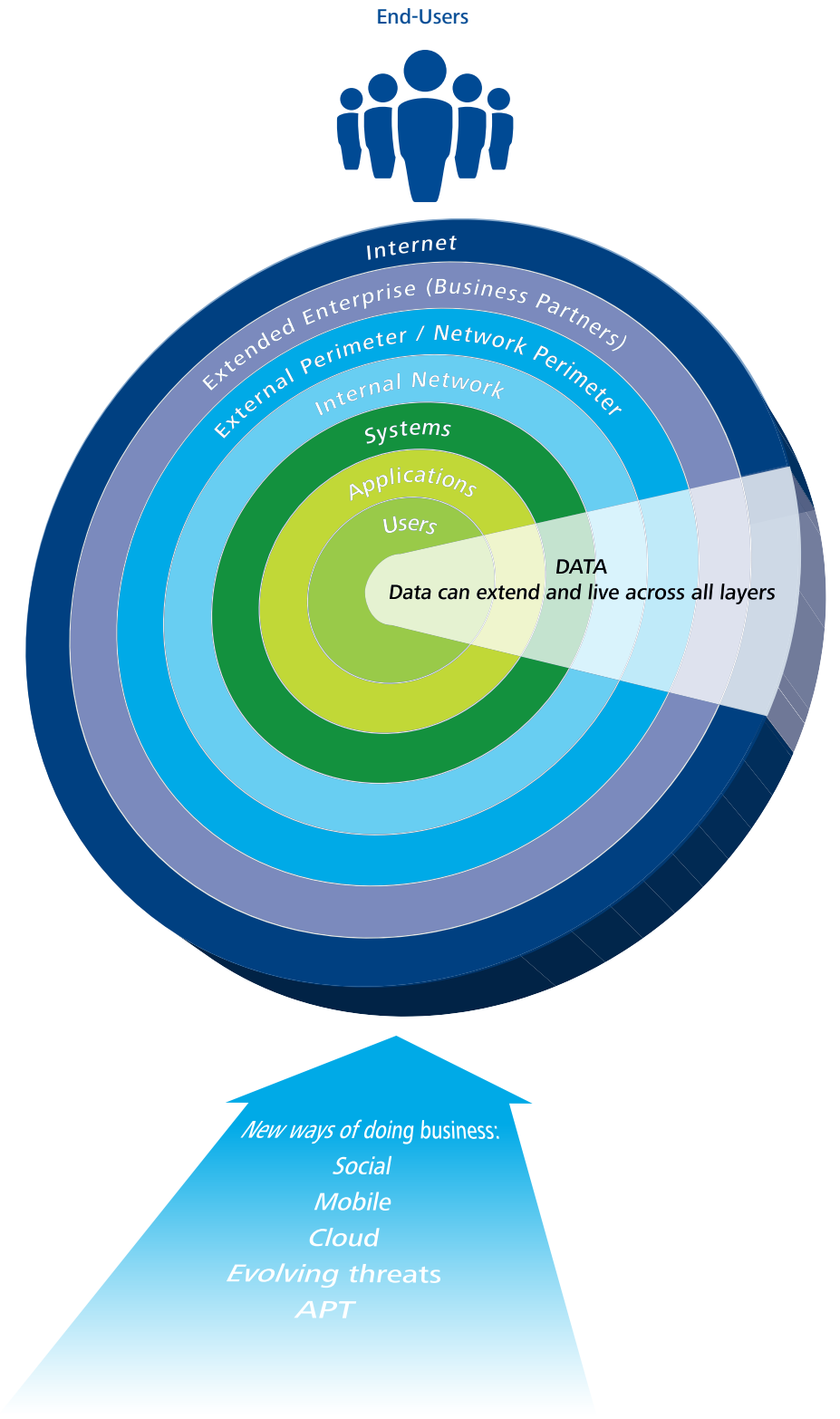
MOVING BEYOND COMPLIANCE AND RAPID RESPONSE

When senior executives approach issues of risk and security, their actions are often shaped by two broad influences. They either adopt a compliance-driven view, reflecting the perspectives of auditors and regulators, or they react to high-profile stories in the mainstream media. Both views are legitimate, yet neither fully addresses the most serious risks posed to organizations.

To make matters worse, the range of threats today is evolving much more rapidly than many enterprise security functions. Mobile devices, social media, cloud computing and other disruptive technology developments have dissolved workplace boundaries, even as they have disrupted the enterprise IT environment. The convergence and rapid evolution of these technologies have transformed the way people and businesses interact in breathtaking new ways and at breakneck speed. It has also changed the way information and personal identity information are

shared and used, often outside the protective umbrella of policies and tools that security people employ.

Figure 2: Data layers



Security, in contrast, has tended to evolve more slowly. Often siloed and organized around compliance, many security functions struggle to implement even the most basic security practices, such as strong passwords, effective user training and workforce awareness. Given the volatile threat environment, security teams can find themselves drinking from the proverbial fire hose, with inadequate resources and limited authority to identify and take on crucial risks.

"There's a deliberate pace of introducing change to large corporate infrastructure," one veteran security professional said. "That pace is controlled by a methodical process of budgets, regulatory requirements and conflicting priorities. Meanwhile, the bad guys can stay as nimble as the speed of technology change allows."

Instead of looking at security risk through a compliance or reactive lens, leaders should take a step back and focus on the basics. Specific strategic choices will vary by sector and company, but the fundamentals apply across all kinds of businesses.

Control. As with financial systems, manufacturing processes or workforce management, *control* is the first fundamental that must be managed. In the case of security threats, that means managing the environment to the extent possible through governance, system updates, automated monitoring, regular cleansing of obsolete data, audit trails and other control mechanisms.

Defend. Layered defense lies at the core of any effort to fend off intruders and threats. It requires building a strong perimeter, supplemented by walls within walls within walls. These measured and progressively restrictive layers of protection allow organizations to focus more resources on securing their highest-value data. The approach should be both preventive and detective, so businesses can monitor security, identify potential threats and deter attacks in real time.

Monitor. Boundaries between companies, their business partners and extended enterprise, and the broader Internet are more porous and more vulnerable to infiltration than ever. Organizations must appropriately protect and monitor critical information transmitted beyond the perimeter to prevent its unauthorized use – whether purposeful or unintentional.

Train. Establish strong, unambiguous policies—backed with ongoing workforce training and development—to ensure that employees understand threats, what actions they should avoid, and how they can proceed in ways that support the organization's strategies and protect its assets. Training and awareness are often the most overlooked of all immediate effective actions an enterprise can

take in the fight against cybercrime. The end user is often the most vulnerable, and this solution is relatively inexpensive to conduct and straightforward to execute.

Prepare. Develop a playbook or response plan that outlines broad mechanisms, tools and strategies for responding to a security incident. Should one ever occur—and it likely will—leadership will not be caught off guard.

As noted earlier, some of the most serious risks today are posed by the growing number of cybercriminals, corporate spies and activist attackers who use a range of simple to advanced techniques to exploit opportunities created by inadequate security. This kind of crime is growing in part because of its low costs and high rewards – big profits with minimal chance of detection.[1] Phishing and the idea that privileged users can be tricked into giving up their credentials to adversaries give credibility to this notion. Relatively uncomplicated attacks can be surprisingly effective. Take, for example, the recent attacks against a sophisticated security solutions company that specializes in authentication, in which adversaries gained access to the company through spear phishing emails.

UNDERSTANDING VULNERABILITIES

Security teams are in the business of managing vulnerabilities that are unique to an organization's businesses, strategies, processes, workforce, IT platforms, supply chains and partners. These risks depend on the value of specific data, intellectual property and systems – and on vulnerability to specific security breaches. Three broad areas of focus form the foundation of most security strategies: access management, software vulnerability management and personally identifiable information (PII) management.

Access management

Access management is the process that allows people (and often applications and machines) to use IT services, data or other assets. Done right, it helps protect the confidentiality, integrity and availability of information by ensuring that only authorized users are able access it. At a simple level, think keys, tokens and passwords which enable access. Yet access management has grown exponentially more complicated.

For example, many users typically log in from one of a few devices and locations, from a specific Internet service provider, with a specific browser or at certain times of day. These attributes can be combined with other variables, such as a

request for a new password or an unusually large transaction, to identify potential incidents. Transactions can be flagged, security teams alerted or additional questions can be posed to suspect users. If an individual fails to meet these challenges, a hold can be placed on the account or the transaction can be declined. This kind of access management is called *adaptive authentication*, and it's quickly becoming tablestakes in today's pervasively connected business environment.

Strong access management policies are among the more cost-effective uses of security resources. They can be automated to reduce the number of incidents and thus the need for responses and damage control. Adaptive authentication is particularly useful now that cybercriminals can gain access by stealing or piggybacking off legitimate users' credentials.

STEPS TO CONSIDER

- **Master the basics.** With basic access management in place, you can then pursue more advanced approaches, such as advanced authentication.
- **Analyze your needs.** Many enterprises that would benefit from improved access management, particularly given the risks of mobile devices and cloud computing, have yet to adopt it.
- **Adapt as you go.** Refine your access policies as you develop new data, adopt new business processes and IT, and identify new user needs.

Software vulnerability management

To understand the nature of software vulnerability, look no further than your own use of electronic devices. If you've ever downloaded an app for a smartphone or tablet, you've demonstrated the challenges that security teams face. Unless you took the time to vet your apps to make sure they're not able to access your calendars, passwords, contacts and browsing history, you've exposed yourself and your organization to potential threats. Even programmers at well established software firms can make mistakes; a simple error or omission by a programmer can leave a system open to exploitation, so keeping up with the latest updates and patches is important. As companies rely increasingly on contingent workers and contractors who access their systems—and as the lines between work and home life continue to blur—the number of software vulnerabilities is increasing.

No antivirus system or firewall can guarantee protection. Hacker enterprises have almost unlimited time, skills and resources to devote to creating and exploiting vulnerabilities. That gives them an advantage over security teams with limited resources and a broad range of priorities. Even leading security companies cannot keep pace with new threats.

Whether they're creating software, implementing solutions or developing in-house systems, IT organizations should be using deep vulnerability assessments,

security design reviews, automated tools and peer reviews. These measures should be applied in the context of cost-benefit analyses. The goal is not perfection, but consistent application of sound risk management practices.

STEPS TO CONSIDER

- **Anticipate and defend.** Anticipating failure enables you to develop damage control, system resiliency, rapid recovery, privacy protection, and notification and public relations plans.
- **Define what's normal to identify what's abnormal.** To monitor for unknown threats, develop heuristics that can detect unusual code or activity.
- **Measure what matters.** Develop baseline metrics and maintain situational awareness of network activity, monitoring for unusual spikes or traffic destinations.

Personally identifiable information (PII) management

The exact definition of personally identifiable information (PII) varies widely across different geographies and industries. In most cases, though, it involves a name combined with an address or some type of identifier, such as a credit card number, bank account number or Social Security number.

The impact of a PII breach can be long-lasting and far-reaching, including loss of data, compliance pressures, customer attrition, diminished trust, dilution of brand equity and negative publicity. Even a moderate breach can result in millions of dollars in emergency response costs, lawsuit defenses, settlements, fines and penalties. Incidents can also violate data privacy laws and trigger investigations by regulatory and law enforcement agencies.

STEPS TO CONSIDER

- **Reduce your "digital exhaust."** Avoid using information that is generally known about you or easily accessible through social websites. When your maiden name or pet's name has been posted on a social media page, it brings security risks. Data can even be aggregated across sites and platforms to understand behavior patterns. For example, it's easy to extract geolocation data from photos to determine where and when they were taken. Similarly, "check-ins" on social media sites can alert others to where you are – and just as important, where you are not.
- **Start with controls.** Managing breaches requires a multifaceted approach to strengthening and improving controls, as well as a breach response protocol. Management is responsible for the specific steps that need to be taken, but make plans to get the board involved, too.
- **Prepare for the worst.** Companies need to be prepared for a wide range of data or information security breaches, but those involving a PII breach are especially sensitive. Your plan should include specific steps for dealing with high-profile publicity and regulator investigations.
- **Go beyond checking the boxes.** There's a lot to do – and no room for cutting corners. Prioritize response actions. Define initial containment activities. Initiate root cause analysis. Develop a remediation strategy and roadmap. Make sure everyone involved knows how to react when security breaches occur – and how to keep them from happening in the first place.

Yet the threat around PII is not limited to data breaches. Cybercriminals don't need access to firewalled data to piece together a profile they can exploit. They can scour the Web for a mother's maiden name or a birth date, compiling more than enough information to ruin almost anyone's day – or worse.

NEW CAPABILITIES, NEW RISKS

At the intersection of today's business, IT and threat environments lie three explosive technologies that come with significant potential risk: social media, mobile devices and cloud services. Security programs that don't focus on these three technologies—and how they are converging and evolving—leave organizations open to new kinds of risks that are only going to intensify.

Social media: Don't "friend" your enemies

Today's social media sites and blogs have created countless new avenues of attack. A Deloitte* survey of technology, media and telecommunications companies showed that "exploitation of vulnerabilities in Web 2.0 technologies" and "social engineering" are regarded as threats by more than 80 percent of the security IT professionals interviewed.[2]

The threat patterns are becoming familiar. Attackers use social media to identify, profile and compile personal data on potential targets. This kind of data aggregation from multiple sites can lead to compromised passwords, data leakage, security incidents and even lawsuits. Criminals can use easily available data to build profiles of executives and board members for identity theft or actual attacks.

From an assault on a global microblogging platform to the infiltration of a politician's email account, determined criminals will usually find a way to reach their targets. They often rely on nothing more than elementary knowledge of technology systems, backed by all the time and patience in the world. While you will not be able to ensure 100 percent security, you can mitigate risks with smart policies and practices.

WHAT WORKS

- **Get proactive.** Understand the features and dangers of social media sites and collaboration tools – and foster awareness of their limitations and risks.
- **Create boundaries.** Establish policies governing the use of social media and collaboration tools. Focus attention on data loss prevention and user education, for starters.
- **Educate your workforce.** Ongoing training is essential to promote the proper use of social media and collaboration tools, and to limit inappropriate data sharing.

* As used in this article, "Deloitte" means Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

Mobile devices: Multiplying avenues of attack

Mobile devices—smartphones, laptops, notebooks and tablets—present relatively easy, low-risk points of entry for attackers who can remotely monitor them for passwords, account numbers, personal data and proprietary company information. As a practical matter, these devices operate outside the control of most businesses today. And even though mobile devices can be outfitted with various levels of protection, poorly planned approaches force trade-offs between ease of use and security. Most mobile devices are not powerful enough to run anti-malware applications while performing other essential applications such as email, phone calls and a calendar. Executives who demand exemptions from security policies for their own personal devices do not help matters.

In addition, many people exercise a lower level of care with cell phones and PDAs, using them for both personal and professional needs. Like it or not, mobile devices are effectively part of the corporate network and should be viewed as such when it comes to benefits and risks.

WHAT WORKS

- **Keep it in country.** Some enterprises restrict users' primary mobile devices to domestic use and issue temporary devices with minimal data for overseas travel.
- **Lock it down.** Configure mobile devices to minimize their chances of being scanned, sniffed or tampered with. Many can be encrypted selectively – whether for travel to high-risk geographies or just a trip to the local coffeehouse.
- **Employ dynamic policies.** Policies such as application white lists are essential. Also, provide workers with guidance as to security capabilities so they can make smarter purchase decisions.

Cloud computing: Overcast with a chance of infiltration

Cloud computing has emerged as one of the most significant IT developments over the past decade, offering new and flexible ways to manage IT costs, scale IT operations and streamline related processes. But cloud also presents new dimensions of complexity relating to information security and privacy, with risks varying significantly with the type of cloud, the architecture and the purpose. When you contract for cloud services, you are handing over critical operations and data to an entity you cannot control or manage.

Every cloud service provider is different. Some limit what customers can inspect, potentially placing the data center and other areas out of bounds. This can spell trouble in a multi-tenant, virtualized world, especially when cloud components reside in foreign locations.

Most enterprises understand the conventions related to domestic cloud service providers, but those in other countries can come with different risks that must be

managed. Other countries may have fewer privacy protections and different views on legal risks, or they may simply take a more lax approach to screening and monitoring employees. In the event your organization needs to produce an audit trail or specific data for tax or legal purposes, you'll need access and capabilities that permit such retrieval.

WHAT WORKS

- **Understand the configuration.** Know where the cloud components and your data will be housed and who is responsible for which functions and risks.
- **Categorize *your* information and operations by risk.** You may be comfortable sharing some functions with cloud providers, but reserve your most sensitive operations for internal use or working with your most trusted providers.
- **Apply *your* standards.** To the extent possible, apply your standards to service providers and business partners. Remember, you can outsource functions – but not risks.
- **Trust but verify.** Due diligence when selecting service providers is a must – as is addressing each party's rights and responsibilities within the contract.

ARE YOU FEELING LUCKY?

With so many issues on the C-suite agenda, it is tempting to relegate security to a compliance function and push proactive planning aside in favor of managing crises *after* breaches occur. Some organizations might even get lucky and escape unscathed with that approach.

But in most organizations the real risk of security threats has captured the attention of boards and executive leadership – and rightly so. Management teams have both fiduciary and legal responsibilities to secure their data and intellectual property on behalf of shareholders. That doesn't mean you need to be a security expert or devote hours to the details of specific security initiatives. But you do need to create a corporate climate that encourages active discussion and proactive management of growing security risks.

For leaders who understand this evolving threat landscape, the path forward is clear. It starts by making a commitment to creating a more secure future – and then taking action to determine what actions make the most sense for your organization. Eventually you'll need to make some hard choices. In the meantime, focus on asking tough questions:

- What are your most important information assets to protect?
- How do you determine the appropriate amount to spend on protecting these assets relative to their value?
- Which areas of your business may be the most vulnerable or desired targets? Of these, which require immediate security improvements?

- What are your data retention policies? When were they last updated? How are you ensuring that your people understand those policies and act accordingly?
- Does your security organization have resources, relationships and systematic processes to investigate emerging threats and rapidly scale resources to remediate a breach?
- Who is responsible for maintaining response plans and educating your executive colleagues about appropriate approaches?
- How are you ensuring that vendors are managing security at least as well as your organization does?

Most organizations can't answer these kinds of questions definitively without cross-functional collaboration driven by C-level sponsorship and engagement. But until the questions are answered, you won't have the guidance you need to make informed choices that balance benefits against costs and risks.

Be sure to keep all three environments—the business, IT and threats—represented at the table. Otherwise, your actions could inadvertently create new vulnerabilities. Business leaders, in particular, have to ensure that plans for moving forward reflect an intelligent approach to managing risk. That won't happen unless there's a shared understanding of the strategic value of data, intellectual property and critical technology systems.

There are tough choices ahead. It certainly doesn't make sense to try and deal with every possible risk on the threat landscape. But it does make sense to ensure that your approach to security is evolving and that you are making appropriate investments that will enable you to address the threats that matter most. **DR**

Ted DeZabala *is a principal with Deloitte & Touche LLP and leads its Security & Privacy practice.*

Irfan Saif *is a principal with Deloitte & Touche LLP in the Security & Privacy practice.*

George Westerman *is a research scientist with the Massachusetts Institute of Technology Sloan Center for Digital Business and the author of IT Risk.*

The authors would like to acknowledge ***William O'Brien*** *of Deloitte & Touche LLP for his contributions to this article.*

Endnotes

1. Cyber crime: A clear and present danger, Deloitte Services LP, 2010 www.deloitte.com/us/cybercrime
2. http://www.deloitteresources.com/dttCDAAttachments/deloitte_-_2009_tmt_global_security_survey_-_findings.pdf