# THE CYBERSECURITY INSIGHT REPORT

Orchestrated by CDW

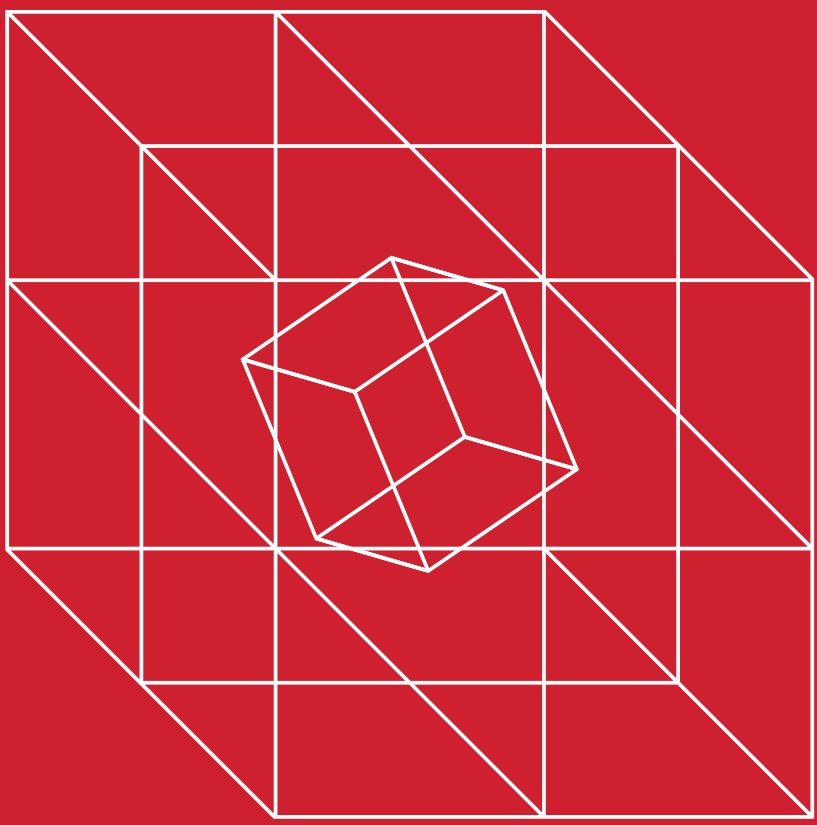

Volume 01

**THE CYBERSECURITY INSIGHT REPORT**
**Orchestrated by CDW**
**Volume 01**



CDW® PEOPLE WHO GET IT®

# WELCOME TO THE CYBERSECURITY INSIGHT REPORT



We have reached a tipping point when it comes to the volume and dynamics of the threats we face. The landscape is not only changing but it seemingly shifts on a daily basis. And to complicate matters further, as the world continues to be increasingly connected, organizations are becoming more vulnerable.

Despite this complicated landscape, one thing is clear: Today, security and business are intertwined. Data and information is now tied directly to profit. Breaches are no longer mere inconveniences. They're not perpetrated by amateurs. And while breach can't be avoided, risk and impact can be mitigated.

What makes cybersecurity so elusive for so many is the shifting nature of risk. Security is a journey, not a destination — and that journey has been made more complex by several factors.

## Threats Are Easier than Ever to Monetize

For all the budding cybercriminals out there, the barriers to entry have never been lower. The advent of cryptocurrency has increased the incentive for anyone with technical skills to become a cyber-criminal. Monetization used to be difficult because law enforcement could follow the money. That's no longer the case.

## Same Old Tricks, Radically New Methods

Social engineering hacks aren't new in principle. These con artist tactics date back to the Middle Ages. And today, those tricks still work.

Many threat actors aren't bothering with finding the next new zero-day exploit when it's so much easier to convince your victim to click. Some serious cases even occur without sending thousands of click-bait emails. These targeted attacks can be as insidious as the following example from a recent incident response: An attacker identified an employee of the accounts payable department. The attacker located that person on Facebook and saw pictures of their children's basketball game. The attacker located the basketball team on the web and downloaded the practice schedule. Then the attacker embedded malware (and a backdoor) into the document, changed a few small details, and sent it to the targeted individual from their child's coach! You may have already guessed — but the victim clicked. The attacker gained access to spend the organization's money, just like that.

The security industry has been talking about social engineering and "spear phishing" for years — but that type of single-click-straight-to-emptying-a-corporation's-accounts-into-a-cryptocurrency-purchase has never been seen before. And it's become both real and pervasive in the last 24 months.

## The Stakes Are Higher than Ever

Today a cyberattack can shut down a business. A single bad actor can drain accounts and hold data hostage. When a business can't make payroll because of a breach, security becomes a much different — and bigger — story.

But it's not all doom and gloom. Because there's so much riding on security, the C-Suite has become involved in the conversation. And with a strong business case, IT is making inroads with a new seat at the table.

The organizations that are most prepared for the shifting cybersecurity landscape are those that understand there is no such thing as prevention, best practices or a one-size-fits-all solution.

**Prepared organizations ask the right questions, they shift their focus to risk mitigation and they develop a strategy that segments their networks and constantly assesses their ongoing risks.**

Cybersecurity will never be easy, and it might seem daunting at times. That's why CDW created this guide. It explores the different ways organizations approach security and mitigate risk. It also presents research and various perspectives from industry leaders across the world. In the end, we hope it helps your organization develop a stronger security posture.

*Sadik Al-Abdulla*
*Director of Security Solutions,*
*CDW*

# Perspectives

Today, cybersecurity resembles an arms race. On one side, threats are evolving while bad actors continue to become more sophisticated and professional with their tactics. On the other, organizations are forced to counter by shifting from a traditionally reactive stance in order to proactively mitigate risk.

It's ongoing. It's daunting. It's confusing. But amidst all of this ongoing change and flux, it is possible to identify major trends impacting the cybersecurity landscape today. We asked some of the best and brightest security minds in the industry to identify some of these trends and how organizations can prepare to meet a new generation of attacks with new technology — and a new approach.

# NOT IF, BUT WHEN. MITIGATING RISK IN THE NEW REALITY.

*by Mark Lachniet*
*Security Solutions Manager, CDW*

Considering that the average data breach in North America costs enterprises a whopping $1.3 million and $117,000 for small and medium businesses[1], respectively, it has never been more important for organizations of all sizes to take the necessary precaution and invest in a comprehensive security plan.

Attacks aren't rare anymore. They are so common, in fact, that if you began installing the latest version of Windows on a live internet IP address without a firewall, you would likely have malware on your machine before it was able to complete its Windows updates.

Unlike the '90s, when hacking was most often performed to establish "street cred" for the hacker or to punish a target, today it's almost always a financial crime. Hacking is lucrative, and that gives bad actors plenty of motivation to apply their formidable skills to penetrate an organization's network. Today, an organization — strike that — any user who connects to the internet is potentially under attack, and the attackers' technology is becoming more and more sophisticated. The result: a Pandora's box of new, ever-changing threats.

The lesson organizations are quickly learning is that threats aren't just inevitable, they're often invisible. Vulnerabilities exist even

[1]https://www.csoonline.com/article/3227065/security/cyber-attacks-cost-us-enterprises-13-million-on-average-in-2017.html

within healthy systems that are "working as intended."

Here's an example. One of the most common practices in Windows shops is to use the same local administrator password across multiple systems. This happens regularly, and for understandable reasons, like easing management overhead or because it's default behavior when provisioning a batch of computers using a disk image.

This one practice has probably allowed CDW's penetration testing team to compromise more systems than any system "exploit" that you might read of in the news. The reason is simple. Once the team gains access to one system — be it an end-user workstation or a server — they can almost always crack or impersonate that local administrator account (or other accounts on the machine) to hack other devices with the same password, and then use it to access even more machines.

Repeat that process a few times and you will almost always end up with domain administrator access. A hacker only needs that initial foot in the door — just one machine — to identify a path to the rest of the organization's systems and data.



## A Daunting Task

There are many similar examples of attacks on fully patched systems that a trained hacker knows well but are rarely found during vulnerability assessments. In an IT industry where organizations struggle with adequate security budgets and training, where new vulnerabilities are discovered on a daily basis, and where attacks are ubiquitous and never-ending, the task of creating a truly secure network is daunting.

With such diversified, lurking threats, how can we guarantee the security of our data and systems? The answer, in short, is that we

can't. Even if we had an unlimited budget and a staff of hundreds of well-educated security engineers, there are still risks (known and unknown) for which we have no reasonable solution. This shift to "when" and not "if" an attack will occur is a fundamental change in the security landscape. A defense-first mindset no longer works. Companies of all sizes must adopt a proactive approach that assesses and minimizes threats in advance while mitigating negative effects when a data breach does happen.

The proactive approach I'm talking about goes far beyond a traditional vulnerability scan or following the rules of a regulation such as Payment Card Industry (PCI) compliance. It requires considering security holistically in a lifecycle that includes continual testing, measurement and improvement.

## Clearing Up the Confusion

In the past, most organizations could perform periodic reviews of their practices and procedures combined with occasional vulnerability scans and consider this reasonable preparation. This is no longer the case.

One of the biggest areas of confusion I see when working with organizations centers on the misunderstanding that exists between vulnerability scans and penetration testing. The fact that there is often no true consensus in the security industry on how to define these two similar activities, not to mention distortions created by imprecise or unethical marketing, does not help to clarify the issue. Both activities are intended to find security risks or vulnerabilities and provide guidance on how to eliminate or minimize this risk. But when done correctly, they provide very different results.

Vulnerability assessments typically involve using a scanning tool to connect to the devices on the network and probe them for known flaws. These tools operate like legacy antivirus systems because they have a pre-programmed set of signatures designed to identify particular flaws.

Scanning is an excellent way to find unpatched servers and devices, but scanning has its problems too. For one, the output of these tools is immense, frequently with hundreds of pages of findings. These findings are usually poorly prioritized, overwhelming to consume and usually don't provide adequate guidance on which issues are the most important to address.

The other problem with vulnerability assessments is that they are almost entirely automated and rarely discover the kinds of "working as intended" problems that a hacker can discover and exploit. Compare this process to penetration testing — the wiser big brother to vulnerability scanning — and the differences can be stunning. A good penetration test does everything that a vulnerability scan can do but adds a significant amount of depth and value by finding issues that are too complex for, or simply invisible to, a scanner. Penetration testing, at least when performed by skilled analysts, can not only identify more problems but present these findings in a far more useful and digestible way.

## The Benefits of Penetration Testing

So why doesn't every organization do penetration testing? The answer is simple and twofold. First, many people don't know the difference between the two. This lack of awareness isn't helped by the fact that many vendors offer "penetration tests" that are no more than vulnerability assessments. They oversell their service, making it seem far better than it truly is.

The second problem is price. Vulnerability scanning is inexpensive, while penetration testing is not. Penetration testing requires extra time by skilled analysts. Again, every vendor will tell you that their engineers are great at security, but how can you really tell the difference?

During my 20 years of security work, it has been my experience that organizations that contract vulnerability assessments are either doing it simply to check the box of some internal or external requirement, or they are driven by the bottom-line cost. To the contrary, those organizations that invest in a true penetration test are those that strive to improve their security and find as many ways to do so as possible.

The same patterns hold true for other security assessments, such as those that focus on practices and procedures or the security of specific applications. Simply put, good assessments require talented engineers and more time. And this can be expensive.

Organizations that routinely conduct in-depth risk assessments such as penetration tests stand a better chance of proactively identifying threats and minimizing damage in the event of an attack because they give a more nuanced view of the environment.

**Good risk assessments are more comprehensive and valuable, and share a few common traits:**

**1. They Are Actionable**
A good risk assessment gives organizations the insight they need to weigh risk and cost. It can also help them manage their risk by choosing to invest in areas identified as being most vulnerable or likely to be exploited in real life. Good reporting reduces the volume of recommendations and focuses on the most important vulnerabilities.

**2. They Are Insightful**
An effective risk assessment will give organizations a deeper level of insight into their systems, identifying threats they wouldn't usually notice — especially if business is running as usual. These insights are difficult or impossible to script and require a well-trained human to discover them.

**3. They Emphasize Skilled People**
Because risk assessments are conducted by humans, they approach systems the same way a hacker would, uncovering risks like password sharing that machines simply can't. Plus, risk assessments give organizations an objective third-party view into their systems.

**4. They Are Comprehensive**
Today more than ever, cybersecurity is a business problem. A good risk assessment approaches threat detection from every possible business angle rather than looking at siloed areas of an organization or its network. Performing tasks such as whiteboarding data flows and cataloging security controls at each stage of a system provide a wealth of information that a quick and dirty assessment cannot.

Sadly, with so much on the line, organizations aren't conducting the right risk assessments as often as they should, if at all. Not only must IT departments fight for dollars, but fear often prevents them from wanting to see what a risk assessment might uncover. Today, organizations need to accept and adapt to the new reality. We're all vulnerable to attack.

You can't prevent a car accident. But you can put yourself in a better position to survive unscathed by learning to be a safer driver and investing in a safer vehicle.

Companies that walk away from security attacks relatively unscathed are those that took the right steps beforehand and have a plan in place to mitigate the impact.

# CHANGING THE CYBERSECURITY CONVERSATION

*by Sadik Al-Abdulla*
*Director of Security Solutions, CDW*

In the wake of breaches that have severely impacted companies like Equifax, Yahoo and Uber to name a few, it's quickly becoming apparent that cybersecurity is no longer an IT problem. It's a business imperative.

From loss of assets and plummeting stock prices, to irreversible reputation damage, it feels like a new threat landscape has begun where breaches are becoming as varied as their potential ramifications.

First, the costs of data breaches continue to rise. According to a newly released Kaspersky Lab survey, small businesses shell out an average of $38,000 to recover from a single data breach.[2] But financial setbacks represent only one angle through which companies must view the prism of cybersecurity.

When a severe breach happens, it can potentially leave a wake of destruction that includes data theft, fines and perhaps more importantly, reputational damage. A recent study issued by CGI and Oxford Economics found that security breaches can permanently erode companies' share prices by 1.8 percent.[3]

To make matters more difficult, there is more incentive than ever for bad actors. Today the rise of cryptocurrency means breaches can be monetized easily, leading

[2] *https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf*

[3] *https://www.cgi-group.co.uk/the-cyber-value-connection-registration*

to an increasing number of criminal groups that each seek financial gain in much different ways and diverse threats. While some focus on credit card information and Social Security numbers, others launder money directly, with cryptocurrency providing an avenue to quickly extort money.

Unfortunately, there is no silver bullet to safeguard against breaches. Prevention isn't the answer. Organizations have never had success stopping attacks. To survive, they need to build a strong internal security culture that mitigates risk. Surviving the accident is what's important, not preventing it in the first place.

Organizations that take a few simple but critical steps have the most success when it comes to implementing a strong security culture.

**Prevention isn't the answer. Organizations have never had success stopping attacks. To survive, they need to build a strong internal security culture that mitigates risk. Surviving the accident is what's important, not preventing it in the first place.**

## Change the Conversation

To build a security culture, organizations must first change the internal conversation from one of breach prevention to risk mitigation. While IT and security staff historically haven't done a good job adapting to the new threat landscape, that conversation is gradually shifting. The evidence is too great to ignore. Today, an IT staff need only point to the recent, high-profile breaches that inflicted crippling ransomware attacks to make their case. Now, the business case for security is met, at least, with an open mind. In the past, investment in security focused on the prevention of threats. Today, when approaching security investment conversations, organizations must think beyond

prevention and focus on breach identification, containment and response while considering their risk model.

**CDW recommends structuring internal conversations around two critical questions:**

1. **How can we prepare ourselves to manage risk and limit the potential damage a breach may have on the organization?**

2. **How can we change our mindset from prevention to risk limitation?**

**Changing the conversation from prevention to mitigation will lay the groundwork for a new security culture.**

## Build a Strategy Around People and Processes

While having the right technology is obviously important, too often companies ignore the people and processes that, in many cases, could have prevented a breach. Technology is limited, and impacting the way users behave has traditionally been outside of IT's realm. When you can't take people away from their desks to talk security and can't manage cultural limitations, it impacts the degree to which IT can affect processes.

## Start Talking About What's Important to Protect

By definition, focusing on one thing means a lack of focus on another. Surprisingly, many organizations fail the most basic step to mitigating risk — identifying the key assets that must be protected in the event of a breach. They view cybersecurity as a one-size-fits-all solution. Instead, think of risk mitigation as a business, not a technology issue.

Start by having a regular conversation with senior leadership, and ask them to identify the biggest business risk that must be dealt with immediately. A simple example is the HVAC management company that featured so prominently in the Target breach. For that organization, the "what to protect" should have been "access to our customers' networks." Viewed through that lens, most technologists would immediately start offering excellent advice.

Regular security assessments from an objective third party can put your security hypothesis to the test and further identify vulnerabilities within systems that, if compromised, would severely impact business. A strong case, backed by financial consequences, is the best way to begin investing in a security strategy that also accounts for people and processes. If organizations don't know where to begin, security assessments can help map and rank the top threats, while informing the people and processes that must be accounted for to mitigate the associated risks.

## View Risk Management As a Journey, Not a Destination

The pace and dynamics of new threats will continue to evolve. Gone are the days when companies can easily fortify their systems. In the face of constantly changing threats, organizations struggle with the often complicated task of keeping pace. Risk management is a journey, not a destination. Rather than becoming daunted by the task at hand, build a strategy by identifying smaller opportunities that you can start now in order to make progress. Create a list, and begin working through vulnerabilities one at a time. With each passing day, risks will become more mitigated, and organizations will be much better equipped to respond in the event of a breach.

# READY OR NOT: REDEFINING ENDPOINT SECURITY TO THWART A NEW GENERATION OF THREATS

*by The CDW Security Solutions Team, with contributions from:*

*Dan Schiappa*
*Senior Vice President and General Manager of Products, Sophos*

*Eric Skinner*
*Vice President Solution Marketing, Trend Micro*

*Michael Viscuso*
*Chief Technology Officer and Co-Founder, Carbon Black*

## Advanced Next-Generation Endpoint Security Must Be Predictive Security

New threats and constant innovation from cybercriminals have put next-generation endpoint security on the "must have" radar for IT leaders. This, plus the expanding attack surface cybercriminals can infiltrate, means the time has come when no organization can be complacent. Businesses must prepare for advanced attacks and understand that they can impact not just desktop, but mobile devices, servers and even the cloud. Today, advanced endpoint security is more critical than ever if organizations want to be prepared for the future.

According to Dan Schiappa, Senior Vice President and General Manager of Products at Sophos, in order to put an effective next-generation security plan in place, IT admins need to assess all the different types of endpoints they might have connected to the network.

"Endpoints today have evolved to include all of the devices employees use in the field to do their job. Adversaries also see servers as just another endpoint, so servers need to be considered just as vulnerable as a desktop computer. Due to the growth in cloud computing, Sophos sees the cloud as a third 'endpoint' that should be protected. The final component to factor in is that the

threat landscape is moving at a rapid pace. Cybercriminals are constantly attacking all of these endpoints using multiple methods and vulnerabilities, from ransomware to zero-day exploits. It is essential that IT admins look at predictive security for endpoints that includes anti-ransomware and anti-exploit capabilities that are enhanced with deep learning technology. This is the definition of next-generation endpoint security today."

## Stronger, from the Outside In

More than ever, cyberthreats are targeting endpoints. The rise in mobility and cloud technology has moved data and applications from outside the traditional protective confines of the corporate firewall. Fluid and constantly evolving endpoints are harder to protect, and hackers see them (and sometimes rightfully so) as an organization's soft underbelly.

To cope, IT professionals are shifting from a primarily reactive mindset to one that's more proactive, adopting new ways of protecting against the sophisticated methods that are weaponizing trusted applications and advanced malware targeted at all vulnerable parts of an organization's network.

"Attacks are becoming polymorphic," says Schiappa. "They are constantly evolving and changing. That's why it is more critical than ever to have endpoint protection that predicts threat behavior and also has additional technologies that block ransomware, detect exploit attacks and provide intelligence to remediate more effectively."

Recent attacks like WannaCry underscore just how unprepared organizations are when it comes to the varying threats posed against their endpoints. This is partially due to a traditional dependence on preparing

for the next "type of attack." Today, to be effective, organizations must adopt security solutions that look for patterns and trends within threats.

## New Technology for New Threats

Artificial intelligence (AI) and machine learning have become key proactive elements to preventing polymorphic cyberthreats on endpoints. In fact, Eric Skinner, Vice President of Solution Marketing at Trend Micro, sees both AI and machine learning as critical components as organizations are forced to continually adapt and evolve.

> **"You have to continue to evolve and learn to combat attacks. AI and machine learning help to detect attacks, especially when they look different."**
>
> ***Eric Skinner, Vice President Solution Marketing, Trend Micro***

AI's unique ability to predict malware used in attacks and then build security measures that focus on the different techniques bad actors are using to infiltrate endpoints can help protect organizations against new threats before they actually happen. With deeper neural learning that's becoming more precise and mainstream every year, AI and machine learning are becoming more granular at simulating the way hackers think. And they're detecting false positives quicker.

## A Sophisticated Response to Sophisticated Threats

While most organizations recognize the increasing need to adapt and respond to endpoint security, many are still stuck in don't-let-me-get-attacked mode. But today, sophisticated threats need a sophisticated response in terms of technology and strategy that embraces endpoint protection without stifling mobility.

For Michael Viscuso, Co-Founder and CTO of Carbon Black, because so few organizations really understand how many endpoints they actually have, focus is (and should be) shifting from protecting endpoints to detection, response and recovery. It's a change that requires a plan that continually adapts.

According to Viscuso, organizations that ask and answer two key questions are usually ahead of the game when it comes to endpoint security.

**Question 1**
**How can we prepare ourselves for the latest attacks?**

**Question 2**
**How can we limit damage when a breach happens?**

To answer both questions, organizations should align themselves with partners and technologies that don't just protect them – but rather keep them one step ahead. This approach is much more than checking a box. Strong endpoint security means growing your predictive capabilities, and it hinges on not falling behind, which requires consistently updating technology. The end goal of endpoint protection isn't just to stay safer today – it's about equipping your organization with the expertise and technology that prepares you for tomorrow.

SOPHOS TREND MICRO Carbon Black.

# THE MORE YOU KNOW: TURNING DATA INTO INSIGHT WITH VISIBILITY

*by The CDW Security Solutions Team, with contributions from:*

*Bobby Guhasarkar*
*Senior Director of Security Product Marketing, Cisco*

*Michael Leland*
*Intel Principal Engineer and SIEM Evangelist, McAfee*

As the cost of cybercrime becomes increasingly intolerable, visibility, both of on-premises networks and cloud applications is requiring more attention from IT decision-makers. In fact, when it comes to evaluating and reporting risk today, greater visibility and transparency is the new norm.

According to Bobby Guhasarkar, Senior Director of Security Product Marketing at Cisco, "Visibility is about understanding the vulnerabilities happening in an environment and then asking, 'Can I do something about it?' It is about knowing what is happening at all times within a corporate network and assets, gathering analytics and taking action against any vulnerabilities that open the door to bad actors."

There's no single approach for providing an advanced level of visibility today. A sound approach that enriches data, and provides actionable insight by ranking the most important events that organizations should focus on has become a critical component of any security strategy.

Michael Leland, Intel Principal Engineer and SIEM Evangelist, McAfee, notes that visibility often has a distinct goal, describing it as a way of "gathering, consolidating, enriching and contextualizing as much security event data as possible. The real goal is to elevate as

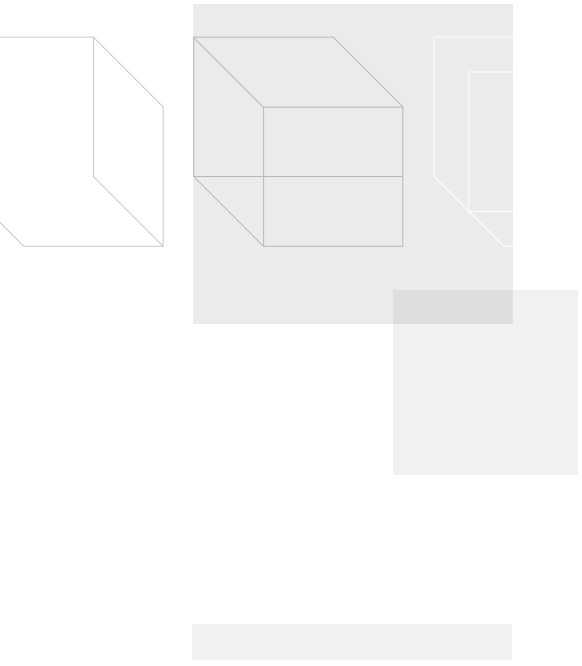
much specific event data and event patterns to the appropriate person with enough information to take action."

**The Five Challenges Organizations Face on the Path to Greater Visibility**

While organizations know that visibility can help them build stronger security practices, there are a number of inherent challenges that prevent them from fully integrating technologies into their organization.

**"Some say visibility is like finding a needle in a haystack. I say it is more like finding the sharpest needle in a pile of needles."**

***Michael Leland, Intel Principal Engineer and SIEM Evangelist, McAfee***



1. **Too Much Data**
   When organizations become overwhelmed with data, they often have a tough time spotting the information that is critical or potentially harmful to their network.

2. **The Knowledge Gap**
   Today there aren't enough people who can handle event data and make sense of it. There are, however, more available tools that can help, like artificial intelligence and machine learning that works behind the scenes.

3. **IT Vendors**
   Organizations want a simple way to understand data without having to do a lot of heavy lifting. But often IT vendors have made solutions too difficult to understand or infer insights.

4. **Short-Sighted Compliance**
   Many organizations feel they can get away with doing the bare minimum by meeting compliance standards. What compliance really does is give a false

sense of security without ensuring protection. It is checking a box rather than solving a problem.

5. **More Endpoints to Protect**
   Organizations have so much to protect today that often small things, like applications that fall outside of their network, slip through the cracks.

With so much to protect and so much on the line, organizations need efficient ways to collect and make sense of data across networks and applications. Thankfully, visibility is adapting to better suit IT needs. Vendors are discovering new ways to segment the most important data, or in many cases, only collecting the data that is deemed most valuable.

According to Guhasarkar, IT can now put software on most endpoints within the organization, giving them much more insight. This software can monitor activity, providing organizations with advanced malware protection. Additionally, vendors can install visibility tools, like Stealthwatch, on network infrastructure attached to Ethernet switches to leverage data across the organization.

**Every organization is at a different place in its approach to risk management. But no matter where they are in the journey, both Leland and Guhasarkar recommend taking a few steps to help increase visibility.**

1. **Recognize the Importance**
   Organizations can't do anything about their overall security until they tackle visibility first. Understanding where you are vulnerable and acting against the biggest risk factors within your systems can help lay a strong groundwork.

2. **Don't Skimp on the Pre-Work**
   According to Leland, visibility starts with the endpoint. If the right data isn't being sent from the right device, your organization might be behind the eight ball. Organizations need to establish the appropriate policies to get event data from the platforms they want. And they also must get the correct intelligence and business context.

3. **Choose a Good Vendor**
   Last, find a reliable vendor that can help you sort through and identify valuable information. It's easy to fall for marketing and hype. Instead, do your research and choose a proven, reputable company.

# A STRONGER SECURITY POSTURE: HOW FOCUSING ON PEOPLE CAN HELP MITIGATE RISK

*by Mike Pflieger*
*Vice President, Enterprise Information Management/ Chief Information Security Officer, CDW*

With the increasing volume and variety of threats such as phishing, malware and social engineering, just one well-educated employee can keep an attack from being successful. In fact, employees can become your first line of defense in securing information assets.

We believe that making security awareness personal helps instill good practices. That's why at CDW, we invest a lot of effort into educating our employees about cybersecurity threats to protect both themselves and the company.

Organizations can't expect each employee to read and understand a comprehensive security policy. They can, however, extract those parts which are important and apply to them. Through targeted communication, training and handbooks, we can educate employees on their specific role-based responsibilities when it comes to protecting data.

A critical misstep we see repeatedly while talking with our peers is that companies focus too much on the "how" instead of the "why." It's easy to talk to employees about safeguards and best practices, but once they understand why, including the ramifications of breaches, engagement and success skyrockets. Good training starts with fostering more interest.

CDW has adopted the carrot approach, rather than the stick, and it's working. We make training easy to understand and navigate, we make it relatable and we reward employees for completing it in a timely manner. We also arrange town hall presentations with the FBI and other agencies to discuss emerging threats and answer employees' questions on best practices for keeping them and CDW safe. The more we can raise the employee's information security awareness, the better protected they and CDW will be.

## THE KEY COMPONENTS OF A STRONG SECURITY POSTURE

**People**

An organization's people are its first line of defense. Conversely, people can also be the weakest link. Employees need to know what to do when faced with a threat. They also need to know how to take preventive measures to prevent malware from impacting the business.

**Process**

Process is knowing the right things to do at the right time. With the right process in place, people can stay productive while your organization keeps bad actors away from critical data and information.

**Technology**

Firewalls and antivirus software used to be the sum total of security, but the landscape has changed significantly over the past decade. With more mobile workers and advancing technology, organizations have had to find new ways to adapt. While technology remains a vital, and most familiar, piece to the equation, it cannot work without the right people and processes in place.

With social media websites like Facebook and LinkedIn, it is easy to research and target the employees with access to the crown jewels within an organization. For that reason, we put special emphasis on educating employees on the specific types of threats that they will face in their role.

How do we ensure our awareness program is working? We use phishing assessment tools to launch internal phishing campaigns to test our employees' security awareness. Some scenarios test general awareness of phishing scams, such as a fake shipping notification or a request to log in to a fake webmail site, compromising your email credentials. Other exercises are targeted to departments with specific access privileges, such as a request to send all the company's W2s to the CFO, perform a wire transfer for the CEO or send a quote for an order that has clear indicators of order fraud.

These tests mimic what we see in day-to-day phishing attempts, giving our employees the opportunity to exercise what they have learned and ensuring that they know how to spot phishing emails. The results of these exercises allow us to measure our effectiveness and adjust our training for employees who might not catch these phishing attempts.

Through these efforts, we have achieved a high level of security awareness in our organization. But we can't stop here, security awareness is an ongoing journey to stay ahead of evolving threats. Making security a part of employees' day-to-day lives results in a solid frontline defense which helps the organization reduce risk.

## Don't Become an Easy Target

Failing to develop a strong security posture makes organizations an easy target for cybercriminals, especially as attacks continue to evolve and become more sophisticated. Bringing people, process and technology together can help mitigate risk while providing the freedom to pursue opportunity.

**To begin developing a strong security posture, consider these three steps:**

1. **Use a framework to organize your security program so that it's easy to communicate outside of information security.**
2. **Decide what the most critical assets are in your organization, understand the risks to those assets and focus your efforts there first.**
3. **Benchmark your capabilities and set long-term goals and priorities to help your organization mature and continually evolve to meet the changing threat landscape over time.**

# SOCIAL ENGINEERING: NEW TAKES ON AN OLD THREAT

*A Q&A with*

*Ryan Kalember*
*Senior Vice President of Cybersecurity Strategy, Proofpoint*

*John Lex Robinson*
*Cybersecurity Strategist, PhishMe*

*Chris Schreiber*
*Consulting Systems Engineer, FireEye*

*Despite accounting for a large (and growing) percentage of hacks, fraud is being overlooked by many CTOs. Weaponized through social engineering, it represents a significant threat to organizations. Today, social engineering attacks aren't just targeting enterprises and small and midsize businesses (SMBs) at higher rates, they're becoming more sophisticated as cybercriminals continue to evolve their methods. We sat down with three experts in the fraud field to discuss these new threats and how organizations can prepare.*

**CDW:** How would you define social engineering in today's IT landscape and how has it evolved over the last five years?

**John Robinson:** It's basically any attempt to manipulate a user into giving you information. But today we're seeing a level of sophistication that we've never experienced before. For cybercriminals, phishing has evolved from a shot-in-the-dark mentality to a professional criminal enterprise.

For example, we used to see emails with grammar errors all over the place. Now you open an email and it looks and sounds professional. Social engineering is now being run like a business. They're targeting individuals. They have moved beyond emails to build entire fraudulent ecosystems online.

**Ryan Kalember:** I see two big factors that define social engineering today. First, the continued rise of email as a business tool has made it extremely easy for criminals to compromise employees. A simple fraudulent email that pretends to come from someone it doesn't has single-handedly affected more companies over anything other than malware.

Second, the cloud has concentrated risk for companies and presented criminals with new opportunities. They can now steal passwords or credentials easier than ever.

**Chris Schreiber:** Social engineering today is a modern twist on con artistry. Today it takes a lot of different forms: email phishing, social, phone and even watering hole attacks where workers are directed to a malware-loaded site to retrieve information.

Con artist techniques have evolved over centuries, but today we're seeing an increasing level of both professionalism and sophistication. For example, today cybercriminals can go out and buy toolkits, complete with customer support, that help them create sites that look identical to something users are very familiar with. The whole operation is becoming more professional and refined.

**CDW:** How are cybercriminals convincing organizations to openly give them information and how are they disguising their attacks?

**John Robinson:** Usually this is happening two ways. First, we're sharing so much online now that cybercriminals have access to a wealth of data that helps them create personalized attacks for individuals because they know where you work, who you work with, etc.

Secondly, they are becoming more skilled at the psychology of persuasion. Humans have a natural desire to be helpful — something that attackers can exploit. Similarly, we're all hard-wired to respond to direction, so they might mimic a boss or a specific coworker asking us to do something very specific. More and more frequently, they're taking advantage of an existing business process.

**Ryan Kalember:** Email spoofing is probably the most common and effective because few organizations actually authenticate email. Criminals are using everyday, seemingly mundane emails with a sense of urgency behind them. For example, they'll get you to click on an invoice. It seems harmless, and that's the goal. You wouldn't think it, but it's also hard to train people not to click on things, so email fraud remains particularly effective. And due to the open nature of the internet, criminals can see when people are moving money and insert themselves into the process with fraudulent methods.

**Chris Schreiber:** Cybercriminals are operating more like businesses. They know how organizations communicate. They're very successful at being able to mimic exactly what an employee would expect to see and do on a legitimate site. And they are also very good at exploiting human instinct. Often, just a casual name drop in an email is enough to convince an employee that it's legitimate.

**CDW:** Why does it seem like organizations are more prone to social engineering attacks than they have been in the past?

**John Robinson:** A lot of this has to do with a change in our society. We're sharing more. Because we've become so comfortable with the internet, our guards are often down. And organizations have given their employees a certain sense of safety and well-being, when nothing could be further from the truth.

**Ryan Kalember:** There are a few reasons. The sheer volume of attacks has grown with more and more tech-savvy criminals operating. And because IT departments are increasingly upping their security game with effective technology, fraud has become

more appealing for many criminals. Also, when it comes to fraud, many companies are relying on a "human firewall," that doesn't understand the threat or the risks.

**Chris Schreiber:** We're always on today – answering emails and communicating digitally. We're also repeating passwords for multiple services. This presents so many more opportunities for cybercriminals to attack, and for users to make mistakes. And because computer systems are all connected online now, organizations have a much greater surface area to protect.

**CDW:** So how can organizations prevent these types of attacks? And what are some of the barriers they will have to overcome?

**John Robinson:** First step, you have to accept that this is an issue. You've got to recognize it and make people aware. Basics like firewalls have to be in place, of course. But also, organizations need to sit down and really look at the assets at risk. What types of data are vulnerable to fraud and how can you protect them?

I also believe that organizations rely on technology and compliance too much. These two factors are check boxes that lull organizations into a false sense of security. A "reasonable effort" is nowhere near enough.

If they really want to mitigate risk, organizations need to understand that it's going to take human intervention. First, understand and recognize the problem. Next, understand the types of attacks out there and the data that's at risk. And then develop capabilities for your users to recognize and report attacks. There's a human factor here that's critical, but it's often overlooked.

**Ryan Kalember:** The movement to the cloud has made organizations more vulnerable than ever. Most security resources are being

concentrated on the network while fraud is happening on the phone, outside of the network. Organizations need to understand how big and far-reaching the threat is. You have to protect your people.

Organizations need to ask themselves what they're most scared of losing and what data is most vulnerable. Next, they need to look at where these attacks are coming from and whether or not they can be fixed. Then, they need to determine a direction and come up with a plan of action.

With the nature of today's connected world, there's also more information available to target individuals. Just heading to someone's LinkedIn profile can give a criminal a good amount of ammo. It's extremely hard to tell people not to put information on LinkedIn.

**Chris Schreiber:** Organizations need to understand the human element at play here. You will never be able to isolate your business to the point where you can prevent these types of attacks from happening. But you can interact with the people you work with and prepare them.

Organizations should look at the most valuable information they need to protect and then determine how their employees interact with that information. Because social engineering attacks are built around the human-to-human exchange of data, a firm grasp of how this occurs naturally can help you build safeguards.

**CDW:** How do you start the conversation with your clients?

**John Robinson:** Usually clients want to build a castle around their data. But you simply can't. I try to help them understand that this is all about minimizing your risk. PhishMe offers training and puts users through the emotional triggers to understand the impact of a phishing threat. We do this around four core areas: simulation, reporting, intelligence and triage.

Our goal is to incorporate what organizations are seeing in the real world and help organizations learn and identify their most vulnerable areas. We want our clients to understand that risk mitigation isn't just about technology. There's a critical human component as well.

**Ryan Kalember:** The first thing for any organization is understanding its threat model. Where are your attacks coming from and what are you trying to limit? You also need to take a good look at your internal processes that might be weak against these types of attacks.

Once you have a clearer sense of the threats, where they're coming from and what you most want to mitigate, you will have a clearer sense of the mitigating technology to deploy.

**Chris Schreiber:** I tell clients that static defenses never work. No matter how high you build your wall, someone is going to eventually get through. One of the first steps I believe organizations should take is shifting the conversation toward building a resilient security program. Organizations need to think holistically in terms of prevention, detection, response and recovery. In other words, build a plan centered around before, during and after attacks.

Next, think of the individuals in your organizations whose access to data pose the biggest risks. Don't forget about training your executives because most of the time they have access to extremely lucrative information. Then develop training and tools that prepare your people against threats.

proofpoint. FireEye

# Key Insights

CDW commissioned the Cybersecurity Insight Report through IDG, the world's leading technology, media, data and marketing services company. Through the course of their research, IDG spoke with over 400 IT leaders about the current state of cybersecurity. From security experts in malware and phishing, to technology and people, their answers have laid the groundwork for a unique insight into the threats organizations face today.

There are seven key insights to help summarize the research. These insights, along with the accompanying research, underscore the current cybersecurity trends, as well as the challenges organizations face. For the complete research, please reference the conclusion of this report.

KEY INSIGHT 1

# MALWARE, VIRUSES, DATA TAMPERING AND UNAUTHORIZED ACCESS TO FINANCIAL DATA KEEP CIOS UP AT NIGHT

Even though organizations should be concerned about these threats, fraud is considered a lesser threat – often ignored – even though it has become the top cause of security breaches.

But more than solely an IT concern, breaches are having a catastrophic effect on overall business with downtime, financial loss and damage to brand and reputation all becoming significant factors.

**50%** of respondents cited malware, viruses and worms as a high cybersecurity risk concern.

**48%** of respondents cited data tampering.

**47%** of respondents cited unauthorized access to corporate financials.

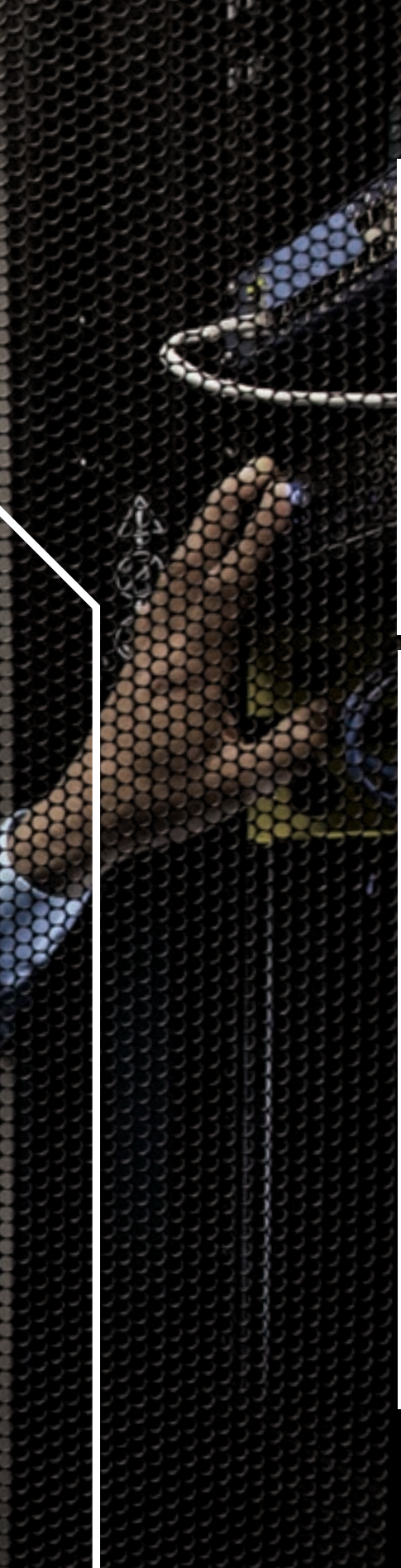
KEY INSIGHT 2

# BREACHES HAVE BECOME MORE COMMONPLACE

Data breaches aren't few and far between anymore. Whether it's due to cyberthreats or employee negligence, sensitive data is being exposed at an alarming rate. More often than not, especially with the rise of malware, organizations might not even know that their systems have been compromised.

**46%** of organizations have experienced a serious security breach.

**22%** have discovered a near-breach in the past 12 months.



KEY INSIGHT 3

# IT STAFFS AREN'T FULLY CONFIDENT IN TECHNOLOGY, PEOPLE OR PROCESS

Contrary to popular belief, a fundamental lack of trust between IT and organizational technology exists. To make matters worse, people and process — often the front line of defense against possible attacks — don't fare much better.

**34%** of those in IT-related positions are extremely confident in technology resources to mitigate risks over the next year.

**30%** are extremely confident in processes and people to stave off cyberattacks.

KEY INSIGHT 4

# BUSINESS IMPACT IS TOP OF MIND

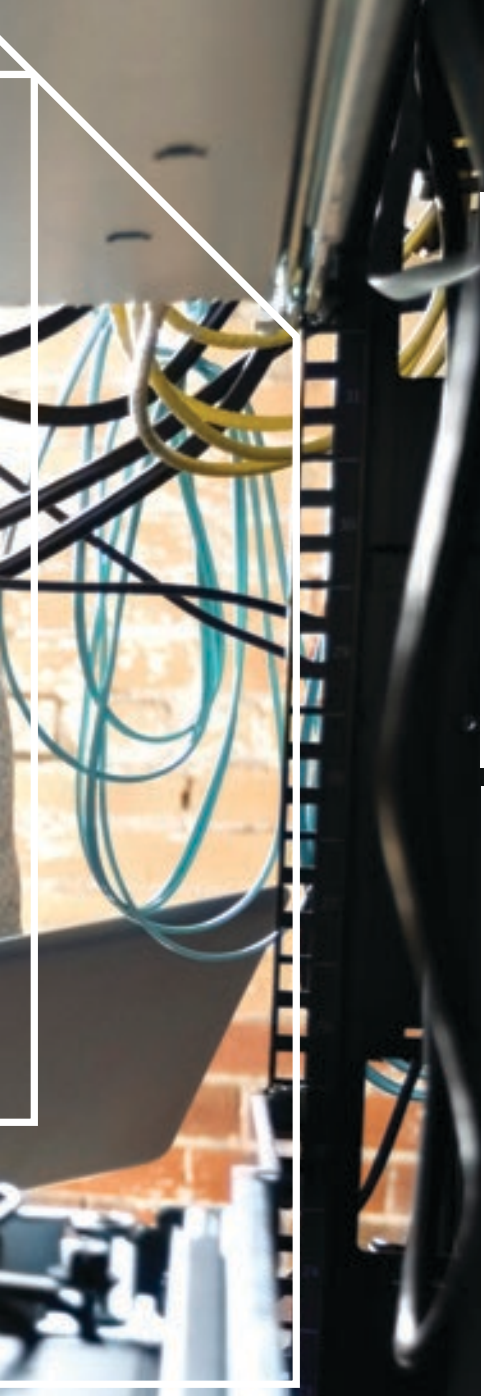
Security threats have shifted in nature, and so have their goals. As cryptocurrency makes monetizing cybercrime easier than ever and as attacks become more sophisticated, one breach can have a devastating impact on the bottom line.

**55%** of organizations regard financial loss and legal repercussions as the most concerning impacts of an attack.

KEY INSIGHT 5

# ORGANIZATIONS ARE DEPLOYING A WIDE VARIETY OF SECURITY TOOLS

When it comes to mitigating risk, there is no silver bullet. To stay ahead of threats, organizations are opting to build and deploy an array of powerful security tools that extend beyond the traditional technology built to solely protect infrastructure.



KEY INSIGHT 6

# ORGANIZATIONS MUST HAVE A DEDICATED SECURITY TEAM

Regardless of size, security has become vital for every business. And because threats have become so pervasive, organizations must consider dedicating a team to protect today's business lifeblood — information.

**68%** of organizations with a dedicated security function are more likely to report an increase in the percent of budget allocated to security.

KEY INSIGHT 7

# NEW TECHNOLOGY CREATES NEW CHALLENGES

From the cloud and mobile workforces to the rise of data analytics, while technology creates new opportunities, it also presents security challenges. Organizations must constantly adapt to keep up.

**44%** of survey respondents cite technology changes as drivers in determining risk management decisions.

# IN CLOSING

As we interviewed IT leaders across multiple industries and researched recent attacks and trends, it has become increasingly clear that to thrive in a threat landscape that continues to evolve, organizations must shift their approach to security. Today, it is no longer a matter of if an attack happens, but when. As such, organizations must abandon traditional defensive postures for proactive strategies designed to mitigate risks and help them quickly recover.

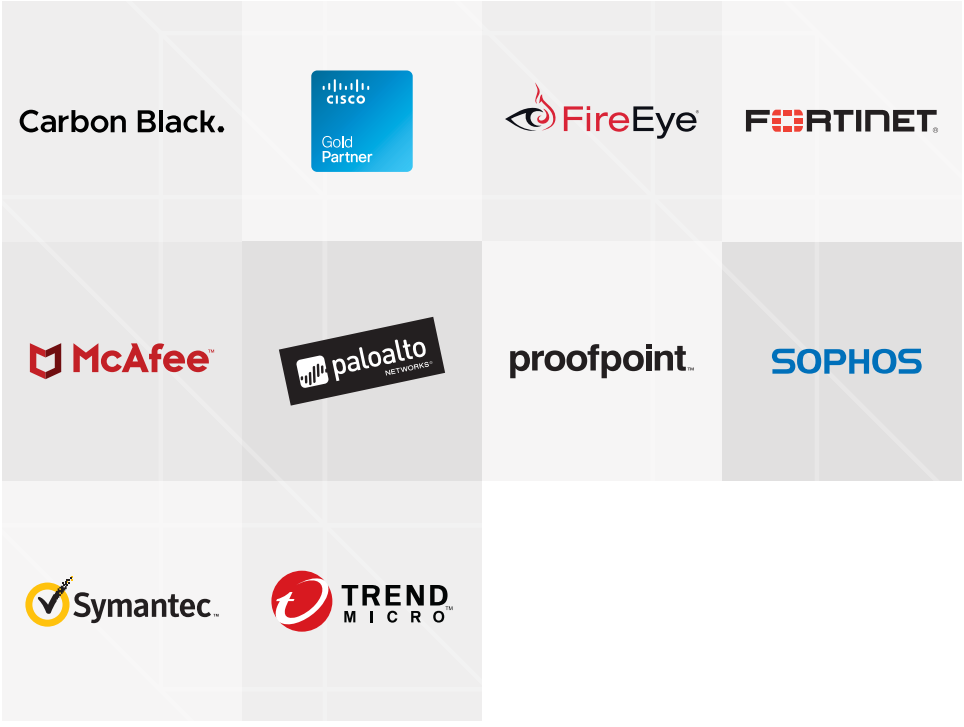
As organizations begin to look at security holistically, they will be better prepared to adapt to a new generation of threats. But that's just the start. Stronger security today means a stronger brand, a more valuable company and more trust during a time when sensitive data has never been more important. As you begin to develop a holistic approach to security, you will be able to prepare, respond and adapt no matter what threats your organization faces, today or in the future.

Working with a wide range of companies and partners across different industries to orchestrate security solutions has given us a unique insight and perspective into the known as well as unknown threats that organizations face today. And we're working hard to bring that collective learning together, so it's easy to understand and implement.

**For more information, interviews and perspectives, we invite you to visit CDW.com/securityreport**

# OUR PARTNERS

The valuable time, research and perspectives that went into making this report wouldn't have been possible without the help of our partners. From assessment, to design and deployment, they represent the best and brightest minds in the security field.

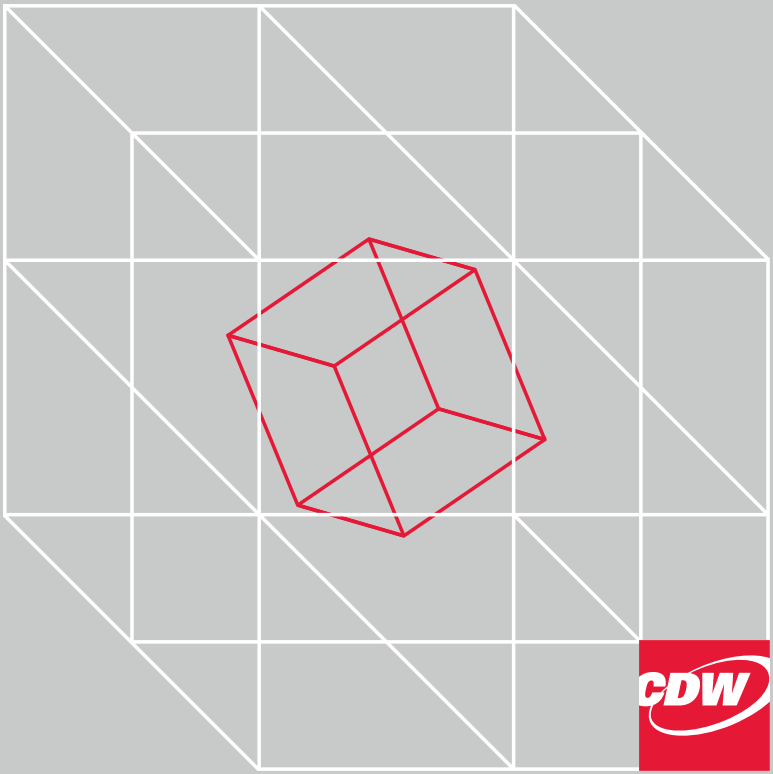



Get an inside look at
the next generation of
threats, and how you
can stay prepared, at
CDW.com/security
CDW
PEOPLE
WHO
GET IT

# THE CYBERSECURITY INSIGHT REPORT

Orchestrated by CDW

## COMPLETE DATA AND ANALYSIS




Volume 01

**THE CYBERSECURITY INSIGHT REPORT**
Orchestrated by CDW
COMPLETE DATA AND ANALYSIS
Volume 01



# THE CYBERSECURITY INSIGHT REPORT

A perfect storm of circumstances is reshaping today's IT security and risk mitigation landscape.

For starters, security threats are more sophisticated than ever. Cyberthieves using malware, viruses and data tampering not only threaten to steal consumer credit card information but take down entire infrastructures, such as power grids, or even disrupt a hospital's life-saving services.

Then there's the sheer volume of data IT teams must protect. By 2020 the digital universe — the data created and copied annually — will reach 44 zettabytes, or 44 trillion gigabytes, according to market research firm IDC. With each new handheld device and embedded sensor, and every new database created, the onus on IT to safeguard sensitive information grows exponentially.

At the same time, the role of IT is changing drastically. Today's CIOs and CSOs must both manage IT security risks and increase operational efficiencies while streamlining business processes, increasing innovation and enhancing customer experiences — all without increasing spending.

The result? A new state of security and risk mitigation, where organizations must adopt innovative strategies — and powerful tools — to circumvent threats and protect confidential data. In an effort to assess the current state of IT security and risk mitigation, CDW partnered with IDG Research to survey 400 senior-level IT security and/or risk mitigation professionals. (For more details on The Cybersecurity Insight Report, see page 22.)

## Key Research Findings

The IDG research study, conducted in late 2017, covered a wide range of topics, from how often breaches occur to the most worrisome consequences of breaches/near-breaches. Among the more revelatory findings:

- **Breaches are common occurrences:** 46% of organizations have experienced a serious security breach, and another 22% have discovered a near-breach, in the past 12 months.

- **IT lacks confidence in technology, processes, people:** Only 34% of those in IT-related positions are extremely confident in technology resources to mitigate risks over the next year. And a mere 30% are extremely confident in processes and people to stave off cyberattacks.

- **Malware tops security concerns:** Half of survey respondents view malware, viruses and worms as their highest cybersecurity risk concern. Interestingly, a lower number (42%) cite fraud as a concern, even though it's the most common cause of security breach (19%) among organizations who have experienced a breach or near-breach.

- **Organizations care most about a breach's impact on business:** 55% of organizations regard financial loss and legal repercussions as the most concerning impacts of an attack.

- **Security tool preferences vary widely:** Organizations are using a wide variety of powerful technologies to mitigate security risks, including Network Access Control (56%), security assessment tools (54%), email security (54%) and traditional endpoint security (54%).

- **A dedicated security team is an organizational necessity:** Organizations with a dedicated security function are significantly more likely (68%) to report an increase in the percent of budget allocated to security.

- **Technology changes create security challenges:** Nearly half (44%) of survey respondents cite technology changes, such as mobile access, cloud shift and Big Data analytics, as the biggest operational challenge in determining risk management strategy decisions.

This report details these key findings and offers strategies for fortifying a security posture in the face of both a changing threat landscape and digital transformation across the enterprise.

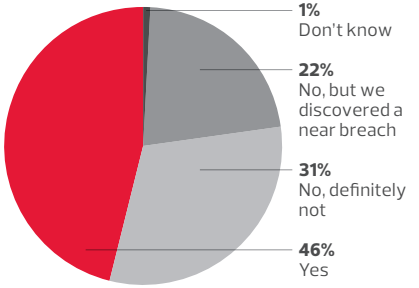
## Confident, But Not Always Prepared

The good news: many organizations are already increasing their investment in cybercrime-fighting tools and implementing savvy strategies, such as regular assessments, monitoring, risk containment and endpoint security.

Despite these efforts though, organizations are not as prepared as they think to combat hackers and minimize human error. More than four in ten organizations (46%) have experienced a serious security breach, and another 22% have discovered a near-breach in the past 12 months, according to the survey findings.

Even though nearly half of organizations have experienced a security breach, and have successfully contained these attacks, it continues to take weeks, if not months, to remediate a breach or near-breach. This is time lost to recovery efforts, rather than prevention.

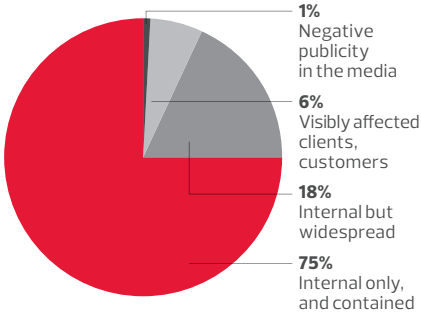
## Has your organization experienced a serious security breach in the past 12 months?




*Source: IDG Research in partnership with CDW*

## Scope of Breach/Near-Breach

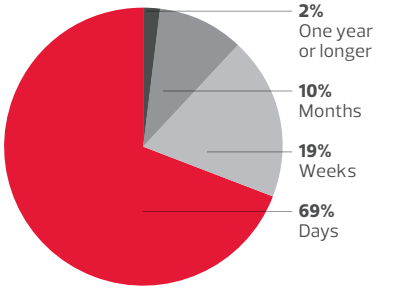
*(Among those who have experienced one)*




*Source: IDG Research in partnership with CDW*

## Time to Remediate Breach/Near-Breach

*(Among those who have experienced one)*




*Source: IDG Research in partnership with CDW*

Large organizations in the finance and manufacturing sectors are more likely to have experienced a breach that had a business and/or financial impact. That's because these sectors rely heavily on the safe storage and processing of highly sensitive data to remain competitive, meet stringent compliance regulations and avoid litigation.

Manufacturers, for example, are increasingly using the Internet of Things (IoT), smart devices, and cloud computing to predict equipment failures, accelerate production cycles, and automate manual processes. Many IoT sensors lack the sophistication for built-in security to begin with; in addition, to keep costs down, some organizations will forgo embedding security into IoT devices and/or providing up-to-date security patches.

Without these patches, IoT devices such as embedded sensors can serve as an entry point for hackers to steal confidential data—or worse yet, take over the functioning of critical equipment.

Consider this example: In tests, researchers at Trend Micro and Italy's Politecnico di Milano altered the operating system of a 220-pound industrial robotic arm, and uploaded malicious code onto the machine from anywhere on the internet. Or this example involving the security of remote surgery, which combines computing, robotics, networks and communications. In a controlled experiment, conducted over a public network, researchers at the University of Washington in Seattle managed to hijack a telesurgery robot, deleting and changing the order of commands it was receiving.

While experiments like these highlight the risks of securing emerging technology such as IoT and robotics, 2017 was a watershed year with an unprecedented number of cyberattacks. Prominent and well-publicized victims include FedEx, Britain's National Health Service, Telefonica and Renault, among others.

And the damages are more far-reaching than ever: last year's cyberattack on credit card company Equifax breached the personal information of 145 million Americans. Among the damages: months of bad press, vanquished customer trust and stolen personal data, including Social Security numbers, credit card numbers and driver's license numbers.

Even tech giants can fall victim to cyberattacks: In 2016, two individuals hacked a third-party cloud-based service used by Uber. The thieves accessed the names and driver's licenses of approximately 600,000 Uber drivers in the U.S. and select personal information of 57 million Uber users around the world. The highly publicized incident prompted many — drivers and passengers alike — to consider competing services.

## Divided Opinion

Another obstacle to cyberthreat preparedness: an absence of consensus between IT teams and non-IT teams on what it takes to properly prepare for threats. Although confidence in current resources to mitigate risk is generally high, those in an IT-related role are more likely to be only "somewhat confident."

Case in point: 62% of respondents to the IDG study who work in non-IT-related positions are extremely confident in technology resources to mitigate risks over the next 12 months. Sixty percent are extremely confident in processes, while 59% are extremely confident in the skills and expertise of people to mitigate risks.

But these high levels of confidence wane within the IT ranks, according to the IDG study. Only 34% of those in IT-related positions are extremely confident in technology resources to mitigate risks over the next year. And a mere 30% are extremely confident in processes and people to stave off cyberattacks.

The differing views between non-IT and IT-related roles may indicate varying degrees of awareness and understanding of today's heightened security risks. Enhanced communication, collaboration and knowledge transfer between these two groups is essential to keeping the digital enterprise secure.

## A Cornucopia of Security Breaches

Despite these differing views on cybersecurity preparedness, there is one thing everyone agrees on: the multitude and sophistication of today's security threats.

Half of IDG survey respondents view malware, viruses and worms as a high cybersecurity risk concern. And for good reason: Last year's WannaCry virus affected hundreds of thousands of computers worldwide. A virulent strain of ransomware, it spread itself across an organization's network by exploiting vulnerabilities in Windows computers. In addition to causing billions of dollars in damages, WannaCry crippled critical facilities, including Britain's National Health Services hospitals.

As threat sophistication increases, the pressure on IT extends beyond handling standard corporate breaches to battling foreign operatives, intercepting stolen government hacking tools and dodging highly targeted cyberattacks.

**Top Cybersecurity Worries**
*(in order of highest concern)*

#1 Malware, viruses and worms
#2 Compromise of customer-facing systems
#3 Unauthorized access to corporate financials
#4 Data tampering
#5 (tied) Ransomware
#5 (tied) Identity theft
#5 (tied) Espionage access to trade secrets

*Source: IDG Research*

Another security concern keeping CIOs up at night: data tampering. Forty-eight percent of IDG survey respondents cite data tampering as a top cybersecurity risk. Healthcare companies are particularly troubled by this type of attack; hacked medical records can fetch a premium on the black market, and stolen patient data can be used to facilitate criminal activities, such as insurance fraud, identity theft and extortion.

For example, last year, in a targeted attack against MongoDB databases, hackers hijacked 26,000 open servers, many of which were used by healthcare organizations to store research data on leukemia patients. The hackers demanded $650 ransom to restore data on more than 200,000 patients.

Other top cybersecurity concerns include unauthorized access to corporate financials (47%), Network Denial of Service (DoS) attacks (45%) and compromised customer-facing systems (44%), according to the IDG findings.

## Common Culprits

IDG survey responses highlight a discrepancy between the most common security concerns, however, and those breaches most likely to occur. Interestingly, a smaller proportion of survey respondents — 42% — cite fraud as a higher concern, even though it's the most common cause of security breach (19%) among organizations who have experienced a breach or near-breach.

However, IT's focus on fraud prevention may intensify as highly publicized data breaches, such as Equifax's, prompt consumers to take actions of their own, such as placing credit freezes on their accounts and setting up fraud alerts.

The second most-cited cause of a security breach among organizations that have experienced a breach or near-breach is malware, viruses and worms (18%). Other common causes of breaches include:

- Data tampering — 16%
- Human adversary and Advanced Persistent Threat — 16%
- Network DoS — 16%
- Unauthorized access to corporate financials — 15%
- Compromise of customer-facing systems — 15%
- Ransomware — 13%

Among companies in the technology industry, data tampering and identity theft are more often cited as the culprits behind a breach or near-breach.

## A High Price to Pay

Survey respondents are also clear on the dire consequences of a cybersecurity breach: more than half — 55% — of organizations regard financial loss and legal repercussions as the most concerning impact of an attack. Indeed, a Ponemon study[1] reveals that the global average cost of a data breach is $3.62 million. Another 54% of survey respondents worry about damage to reputation.

[1] *Source: 2017 Ponemon Cost of Data Breach Study*

**Most Worrisome Consequences of Security Breaches**

*(in order of highest concern)*

#1 Legal consequences
#2 Financial loss
#3 (tied) Damage to reputation
#3 (tied) Downtime or outage
#4 Drop in shareholder value

*Source: IDG Research in partnership with CDW*

Industry sector plays a significant role in determining levels of concern among organizations. For example, 51% of overall IDG survey respondents say government or regulatory obligations or consequences are concerning. As expected, this figure is higher among healthcare companies as they must meet stringent regulatory controls, such as HIPAA, or risk facing steep fines.

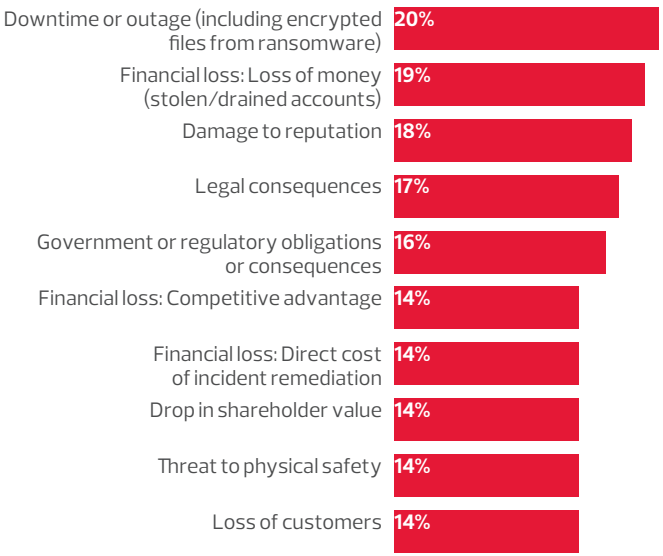
Similarly, of the 38% of survey respondents that report threats to physical safety as a concern, manufacturing companies are most highly represented. These days, many factory workers perform side by side with collaborative robots. These powerful machines are often embedded with sensing technology so that if a human comes too close during operation, it will automatically stop whatever it's doing. That is, provided the manufacturer's network hasn't been hacked.

## On the Outs

Financial loss and legal repercussions may top organizations' security concerns, but they are overlooking one of the more common real-world consequences of a breach: the majority of survey respondents – 20% – cite downtime as the most common consequence of a security breach, closely followed by financial loss (19%), damage to reputation (18%) and legal consequences (17%).

**Resulting Impacts of Breach/Near-Breach**

*(Among those who have experienced one)*




*Source: IDG Research in partnership with CDW*

That's surprising given the significant impact downtime can have on an organization's critical operations, especially in today's fast-paced, highly competitive global economy. Examples range from momentary manufacturing delays to widespread outages such as the cyberattack that wiped out power across parts of the Ukrainian capital, Kiev, last year.

And the cost of downtime can be staggering: According to a 2016 survey[2] from Information Technology Intelligence Consulting, 81% of respondents said one hour of downtime cost their businesses more than $300,000, while 33% said that same 60 minutes of downtime cost their organization between $1 million and $5 million.

## Top Strategies for Mitigating Risks

To improve their cybersecurity risk posture, organizations are turning to a wide variety of powerful technologies. Among survey respondents, more than half have already implemented Network Access Control (56%), security assessment tools (54%), supplementary email security (54%) and traditional endpoint security (54%). What's more, close to a quarter are considering these same technologies: Network Access Control (23%), security assessment tools (20%), email security (21%) and endpoint security (24%).

And as the security landscape evolves, organizations are slowly adding new and innovative technologies to their security toolkit. For example, 30% of IDG survey respondents are considering technologies that monitor user behavior (User and Entity Behavior Analytics) to improve their cybersecurity risk posture.

User and Entity Behavioral Analytics (UEBA) works by monitoring patterns of human behavior, then using algorithms and statistical analysis to identify anomalies in patterns that may indicate a potential security threat. Early adopters of UEBA are still working on minimizing the number of false positive alerts of cyberattacks. But as the behavior rules integrated into these tools become more refined, accuracy rates are likely to improve.

Next-generation endpoint defense is also piquing interest among security-minded organizations. Thirty-nine percent of survey respondents are considering these technologies, which combine machine learning, threat intelligence and behavioral analysis to thwart sophisticated attacks and protect both the endpoint and enterprise network.

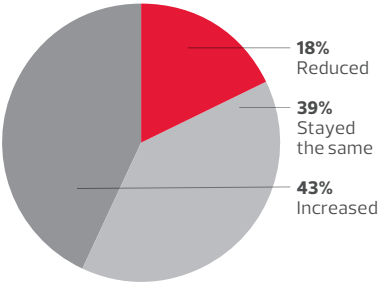
For years, organizations have relied on traditional security tools to protect their networks from hackers. That's changing as mobile workforces expand. But while some fear next-generation technologies can introduce new security risks, others believe these same technologies can also help reduce threats before they happen.

## Budgetary Concerns

From traditional security tools to next-generation technologies, organizations are putting their money where their mouth is: The proportion of IT budget allocated to security and risk mitigation is on the rise at more than four in ten organizations (43%), according to the IDG survey. But not all organizations are investing — 39% of respondents' IT budget has stayed the same over the past two years.

[2] *Source: Information Technology Intelligence Consulting*

## Change in Proportion of Budget Allocated Towards Security and Risk Mitigation — Past 2 Years




Average increase: 19%

*Source: IDG Research in partnership with CDW*

Who — and what — drives IT leaders to purchase cybersecurity tools varies by organizational structure, experience and title. For instance, organizations with a dedicated security function are significantly more likely (68%) to report an increase in the percent of budget allocated to security, according to the IDG survey. However, at companies where security falls under IT's purview (66%), the allocation has typically remained flat — an indication that IT teams may lack the authority to influence budgetary decision-making.

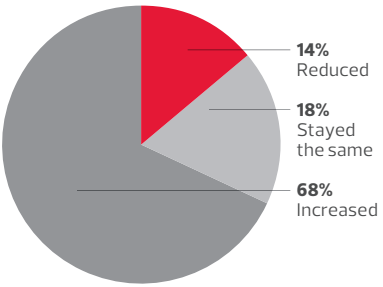
History also dictates the degree of commitment to cybersecurity. Organizations that have experienced a breach are more likely to report an increase in security budget allocation over the past two years. At the same time, respondents with non-IT titles are more likely to report an increase in budget compared to their IT counterparts — again, a possible indication of IT's limited say in budgetary decision-making.

### Barriers to Safeguarding Data and Operations

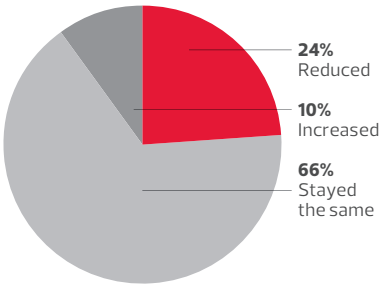
Technology is forever changing the way people work, businesses operate and industries evolve, often for the better. Smartphones and wireless networks can create fast-acting, collaborative mobile teams. Cloud computing enables organizations to process and store vast volumes of data for a fraction of the price of on-premises servers. And industries

## Change in Proportion of Budget Allocated Towards Security and Risk Mitigation — Past 2 Years

**Dedicated Security Function**




**Security Is Combined with IT**



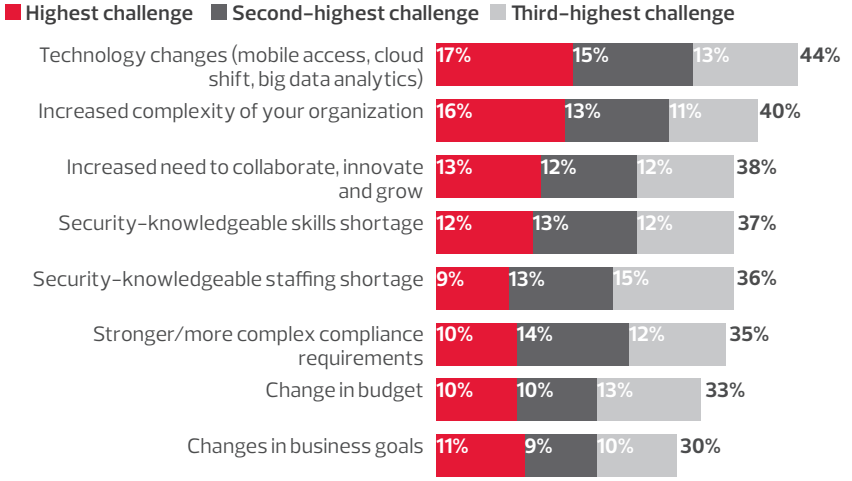

*Source: IDG Research in partnership with CDW*

from manufacturing to healthcare are analyzing treasure troves of data to improve business processes. But for all its business benefits, new technology and the resulting organizational change can exacerbate the difficulty of developing and executing a security and risk-mitigation strategy.

Nearly half (44%) of IDG survey respondents cite technology changes, such as mobile access, cloud shift and Big Data analytics, as one of their top three operational challenges in determining risk management strategy decisions. Forty percent cite the increased complexity of an organization as a top-three obstacle to decision-making. And 38% of survey respondents rank the increased need to collaborate, innovate and grow, which makes risk mitigation more difficult, among their top three challenges.

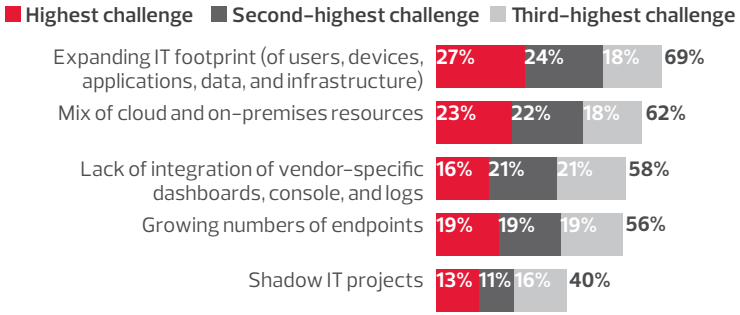
Technology complexities are also complicating cybersecurity efforts. Nearly three-quarters (69%) of respondents rank IT's expanding footprint — users, devices, applications, data and infrastructure — as one of their top three technology-related challenge to determining risk-mitigation strategies. Another 62% rank hybrid environments, such as a mix of cloud and on-premises sources, as a decision-making road block among their top three challenges. And 58% say their top three challenges include a lack of integration of vendor-specific dashboards, consoles and logs as getting in the way of a risk mitigation plan.

**Biggest Operational Challenges in Making Risk-Mitigation Strategy Decisions**




*Source: IDG Research in partnership with CDW*

**Biggest Technology-Related Challenges in Making Risk-Mitigation Strategy Decisions**




*Source: IDG Research in partnership with CDW*

An organization's structure can also impact cybersecurity efforts, especially when it comes to budgeting for initiatives. For instance, 33% of survey respondents say change in budget makes it harder to develop a risk-mitigation strategy. And 30% of survey respondents report changes in business goals as obstacles. Interestingly, the majority of these respondents are most likely to work at organizations with a dedicated security function.

One possible explanation for this is that a dedicated security function is more likely to have a seat at the C-suite table than rank-and-file IT professionals. As a result, changes in budget and business goals can have a direct impact on the team's efforts to establish risk management strategies, especially if these initiatives require an increased IT budget or greater access to corporate resources.

## Balancing Prevention with Proactivity

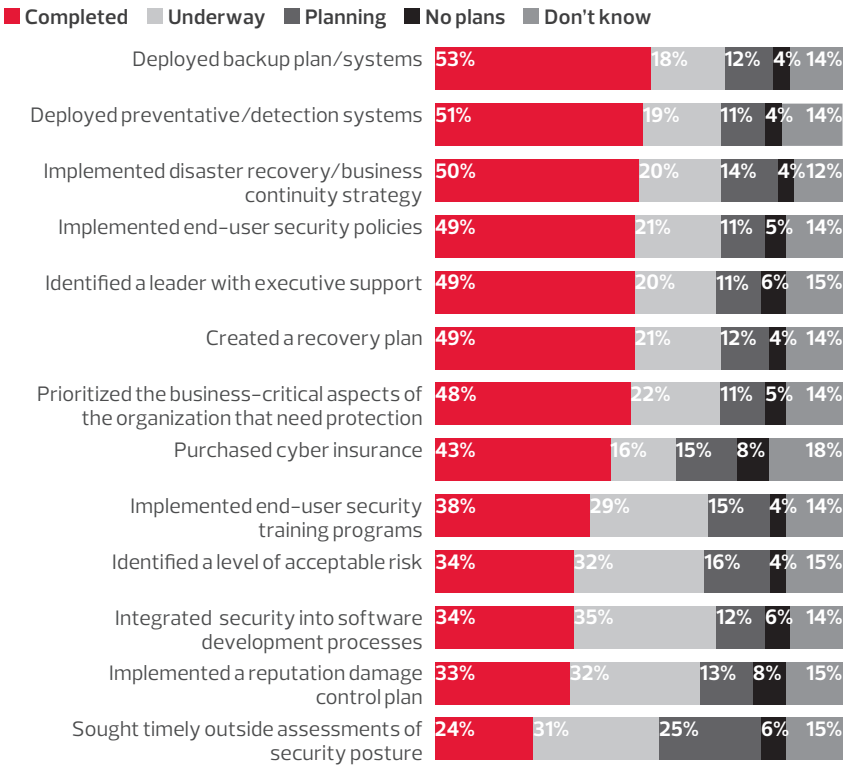
To overcome the technological and organizational challenges of developing a security strategy, most organizations are adopting a better-safe-than-sorry approach to cyberthreat prevention. For many, this involves using technology tools to uncover potential breaches before they occur.

For instance, 53% of survey respondents have fully deployed backup plans and/or systems to improve their security posture. Others have fully deployed preventive and/or detection systems (51%), as well as disaster/recovery/business continuity strategies (50%) to identify and mitigate risks. Another 18%, 19% and 20% have plans for these same technologies underway, respectively, according to the survey.

Policies and people also feature prominently in organizations' efforts to thwart cybersecurity attacks. Employees are one of the leading causes of data breaches today; malware often enters an organization via phishing or social engineering attacks in which an employee unwittingly clicks on a malicious link or download.

To curb employee negligence, 49% of IDG survey respondents say they have

**Measures Taken to Improve Organization's Security Posture**




Organizations with a dedicated security function are more likely to have already taken each of these measures.

*Source: IDG Research in partnership with CDW*

implemented end-user security policies, another 21% say such policies are underway and 11% say they are planning to implement these tactics.

In addition, 38% of IDG survey respondents have implemented end-user training programs, another 29% say such programs are underway and 25% are planning to use end-user training.

**Tactics to Thwart Security Breaches**

**IT and security professionals:**

- Make sure all end-user devices — personal and corporate — are password protected, and enforce strong password policies
- Employ multifactor authentication (MFA) where possible
- Install a complete antivirus software on every device

**Employees and users:**

- Avoid opening email attachments, clicking on links or downloading files from unknown sources or with questionable content
- Always check the email and names of correspondents prior to opening a message
- Manage passwords properly, including changing them regularly
- Never share confidential information over a public network

In addition to establishing stringent end-user policies, 49% of IDG survey respondents say they have identified a leader with executive support to champion security efforts across the C-suite and advocate for greater security measures. An additional 20% and 11%, respectively, have this type of strategy underway or in the works.

## Methods of Assessment

Close to one-quarter (24%) of IDG survey respondents have already put a strategy in place for timely outside assessments of their security posture, and another 31% say plans for such assessments are underway.

"Make sure you have a third party testing your security posture," says one survey respondent. After all, the right third party can provide an objective perspective on an organization's cybersecurity preparedness and identify vulnerabilities that internal teams may have missed.

Information gathering is also key to flagging and assessing threats before they occur. However, opinion is divided as to which tools provide the most accurate intelligence: 35% of respondents identify and assess cyber-security vulnerabilities using information from patching or antivirus tools, while the same percentage rely on information from Windows Update or inventory management tools.

As expected, less popular approaches to identifying and assessing cybersecurity vulnerabilities involve more labor-intensive activities. The reason is simple: Today's IT teams are strapped for time and short on resources. Heavy lifting to conduct threat assessments takes away from more mission-critical tasks. For example, only 26% of survey respondents use tools such as Microsoft Security Baseline Analyzer and Microsoft Operations Manager to self-scan for vulnerabilities. Self-administered penetration tests (which require extensive hands-on work and analysis) also rank low (20%) as a preferred approach to identifying cybersecurity vulnerabilities.

## Compliance Raises the Stakes

Although preventative measures are critical to staving off cyberattacks, many organizations are embracing a more proactive approach to risk mitigation as a result of today's changing and intensifying regulatory environment.

Thirty-seven percent of IDG survey respondents work to identify cybersecurity vulnerabilities in their organization's practices and procedures as meet compliance regulations, such as PCI, HIPAA and NIST 800-53. According to one survey respondent, "Compliance is key."

### How Organizations Identify and Assess Cybersecurity Risks

| | |
|---|---|
| Identification of weaknesses in the organizations practices and procedures when working to comply with regulations such as PCI, HIPAA, NIST 800-53, etc. | 37% |
| Information from patching or antivirus tools | 35% |
| Information from Windows Update or inventory management tools | 35% |
| Self-scanning for vulnerabilities (e.g., using Microsoft Security Baseline Analyzer, Microsoft Operations Manager, or System Center Configuration Manager) | 26% |
| Alert by an employee or outsider | 25% |
| Information from periodicals, partners and newsletters | 25% |
| Self-administered penetration tests (extensive hands-on work and analysis) | 20% |
| Self-scanning with other tools to assess specific or complex technologies like web applications | 20% |
| Self-scanning for vulnerabilities using security tool (such as Tenable's Nessus, Rapid7's Nexpose) | 18% |
| Contracted audits or gap analyses with regulatory standards such as PCI, HIPAA, NIST-800-53 to identify security risks | 16% |
| Contracted vulnerability scans (minimal hands-on work and analysis, lower cost) with a third party | 14% |
| Contracted penetration tests (extensive hands-on work and analysis, higher cost) with a third party | 14% |
| Contracted scanning with other tools to assess specific technologies like web applications | 13% |
| Other | 1% |
| None of the above | 2% |

*Source: IDG Research in partnership with CDW*

It's easy to understand why compliance is a catalyst for greater security: Failure to meet regulatory mandates and their security requirements can result in the loss of the ability to accept credit cards, sweeping legal liabilities and hefty government fines, among other things.

In fact, 51% of survey respondents say compliance and regulation mandates are key drivers in promoting them to take proactive action to avoid cybersecurity breaches. Other external factors driving greater diligence include:

- Executive mandates — 47%
- Large publicized security events — 46%
- Peers that have been breached — 46%
- Industry and function-related education sources — 37%

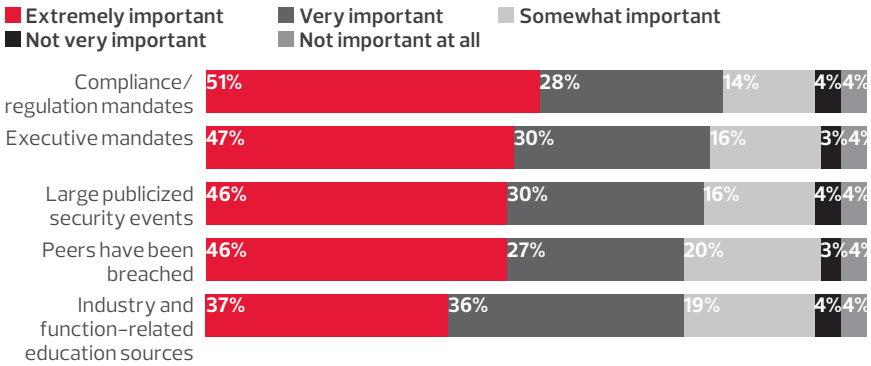
Together, these factors are pushing organizations to up the ante on their risk-mitigation initiatives.

## The Bottom Line

With technology stacks growing and compliance regulations tightening, IT leaders must move beyond simple preventative measures. Adding urgency to the matter are increasingly sophisticated cyberattacks, expanding data volumes and new responsibilities for IT leaders.

But while the tools exist to mitigate security risks, survey respondents indicate the need for changes in people, processes and organizational structure. A dedicated security function can help by securing C-suite support — and budget — for more complex risk-mitigation strategies. A proactive stance against imminent threats can shield an organization from the legal liabilities, productivity losses and reputational impact of a highly publicized breach. And greater external support can provide organizations with the objective perspective and expertise needed to truly steady themselves for today's new state of security.

**Importance of External Drivers in Prompting Organizations to Take Action Before Becoming Victimized**



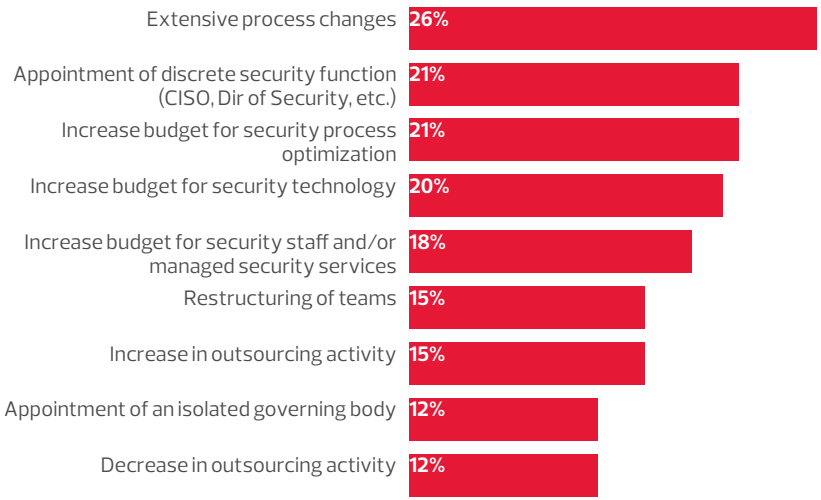

*Source: IDG Research in partnership with CDW*

# LESSONS LEARNED FROM THE IT SECURITY TRENCHES

Security breaches are known for producing sleepless nights — and may even result in termination, depending on the severity of the breach — but they can also bring about positive changes in security and risk-mitigation policies, procedures and culture.

**Impact of Breach/Near-Breach Operationally**

*(Among those who have experienced one)*




*Source: IDG Research in partnership with CDW*

More than one-quarter (26%) of IDG survey respondents that have experienced a breach have made extensive process changes as a result. Others have been prompted to appoint a discrete security function (21%) or increase budgets. Those budget increases include finding or freeing up funds to invest in security process optimization (21%), security technology (20%), and security staff and/or managed security services (18%).

Today's CIOs and IT security professionals can take a page from these organizations. Here's what every IT security and/or risk mitigation professional should consider when developing a risk management plan.

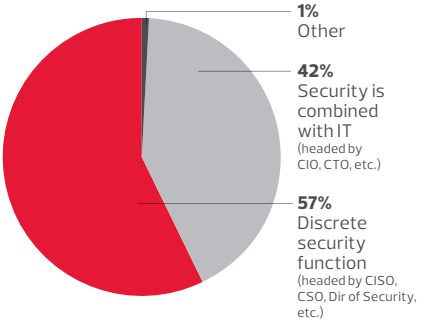
**1. Establish a dedicated security function**

More than half of IDG survey respondents (57%) have a discrete security function in place that is not combined with IT. Headed by a CISO, CSO or director of security, this team is primarily responsible for developing and enforcing cybersecurity policies and procedures.

But not all organizations can (or want to) allot human capital and IT resources to a dedicated security function. In fact, 42% of survey respondents report that their security function is combined with IT and led by a CIO or CTO.

According to the survey findings, that's a missed opportunity to bolster IT budgets and boost cybersecurity preparedness. For instance, organizations with a dedicated security function are significantly more likely (68%) to report an increase in the percent of budget allocated to security, according to IDG survey respondents. Conversely, at companies where security falls under IT's purview (66%), the allocation has typically remained flat, or worse yet, experienced a 24% reduction in budget allocation.

**Primarily Responsible for Developing and Enforcing Cybersecurity Policies and Procedures**




*Source: IDG Research in partnership with CDW*

Organizations with a dedicated security function are also more likely to have already taken cybersecurity measures by establishing backup plans, deploying disaster recovery solutions and designing business continuity strategies.

Given its advantages, it's no wonder that survey respondents in larger organizations, as well as those in the finance and manufacturing sectors, are more likely to report that they have created a discrete security function.

**2. Have a plan for acting quickly — time is of the essence**

Nearly one-third (31%) of respondents report it took a period of weeks or longer before they were able to remediate a security breach or near-breach that occurred. One survey respondent admitted: "We need to be more forthcoming about a

breach and its details — total transparency." Unfortunately, a slow response can significantly increase the impact and severity of a breach. Financial impact, regulatory or compliance fees, loss of customers and negative brand impact are likely to grow (and increase the total impact) as a breach lingers.

But there are ways organizations can plan to minimize the damages of a security breach. Putting disaster recovery tools in place can help restore services quickly. But technology is only one piece of the remediation puzzle. A predetermined response plan is also critical to limiting exposure to security breaches. Key components of a plan are as follows:

- Identify the cause of the breach, contain it and install the necessary patches.
- Assess the damage: What systems have been affected? How many users have been impacted? What data has been stolen?
- Team up legal and IT professionals to quickly assess potential exposure to liability, contact regulators and advise on next steps.
- Ensure the emergency response team is meeting all the necessary legal obligations.
- Immediately report the incident to affected clients and government authorities within the prescribed time.
- Know who to contact — and how — to speed up the remediation process and enable IT to focus on more critical tasks, such as containing the breach.
- Advise employees to reset passwords on accounts that may have been compromised.

Despite the steady stream of headlines chronicling worldwide cybersecurity attacks, most organizations manage to keep their security breaches under wraps. Other than required regulatory disclosures, the vast majority (75%) of IDG survey respondents say they contained awareness of a breach or near-breach internally.

Only 6% reported a breach as having visibly affected clients or customers, and a negligible 1% of survey respondents admit to receiving negative publicity in the media as the result of a breach or near-breach.

**3. Budget appropriately for security**

IT budgets earmarked for security and risk mitigation are on the rise at more than four in ten organizations (43%), according to the IDG survey. Yet, at the same time, 39% of survey respondents say IT budgets have stayed the same over the past two years.

There are a number of ways organizations can secure more funding for risk mitigation. For one, an internal security champion or advocate with access to the C-suite can significantly influence budgetary decisions; the task shouldn't be left to IT teams alone to handle. Similarly, as previously noted, survey findings reveal that organizations with a dedicated security function are more likely to report an increase in the percent of budget allocated to security.

One of the rare upsides of a security breach is that it can spur organizations into action. Case in point: 18% of IDG survey respondents who have experienced a breach have increased budget for security staff and/or managed security services.

**4. Implement technology that provides better visibility and predictions**

Many organizations are dangerously taking more of a reactive than proactive approach to mitigating risks.

Although one survey respondent advises organizations to monitor their systems "consistently," IT leaders must also identify and assess threats before they occur. The right tools can help: 35% of IDG survey respondents identify and assess cybersecurity vulnerabilities using information from patching or antivirus tools, and the same percentage rely on information from Windows Update or inventory management tools. Vulnerability scans can also play a part in early threat detection.

**5. Engage with trusted third-party partners**

As today's security landscape evolves, survey respondents sense a growing "need to hire external security expert resources." No longer can IT teams simply deploy risk-mitigation tools and technologies. Rather, mobile technology, cloud computing and data analytics are creating complex IT infrastructures. At the same time, an expanding IT footprint and hybrid environments are challenging IT leaders to determine risk management strategies.

A third-party partner can help organizations overcome these technology and organizational challenges by delivering a potent mix of tools and expertise, while also providing a broader focus on cybersecurity risks. For many organizations, hiring a third-party partner with specialized expertise in security is well worth the investment.

In addition, specialized third-party partners can help organizations stay abreast of changing compliance and regulations (especially in heavily regulated industries), help assess and monitor third- and even fourth-party vendor security risk and more.

Respondents clearly see the value of strong partnerships. Among survey respondents who have experienced a breach/near-breach:

- 18% — Increased budget for more staff and/or managed security services
- 15% — Restructured teams
- 15% — Increased outsourcing activity

**6. Implement (and evolve) end-user training — and communicate processes and changes**

"Training and awareness of threats" are critical components of any security toolkit, says one IDG survey respondent. Currently, IT teams are largely responsible for creating and enforcing cybersecurity policies and procedures.

Keep in mind that these policies and procedures must evolve as new regulations and compliance requirements emerge. It's up to IT to stay abreast of these changes and alter their security strategies accordingly, then communicate those changes to end users, third parties, customers and so on.

Seminars, workshops and online training modules can teach end users how mobile devices and IoT possibly create new entry points for hackers. Education initiatives can also drive greater adoption of end-user protocols, such as deploying security patches and updating software, by teaching employees that increased security is in their own best interest.

### 7. Extend security responsibilities to business and legal teams

Along with existing security teams, IT is largely responsible for creating and enforcing cybersecurity policies and procedures. In fact, 63% of IDG survey respondents report IT management handles the development, application and enforcement of cybersecurity policies and procedures. Another 28% cite IT staff as responsible, while 20% point to IT consultants as a key part of a wider security team.

Respondents whose companies do not have a discrete security function indicate that cybersecurity policies and procedures are typically shared across an average of three roles.

**Wider Team Responsible for Developing and Enforcing Cybersecurity Policies and Procedures**


Respondents whose companies DO NOT have a discrete security function indicate these responsibilities are typically shared across multiple roles (3 on average).

*Source: IDG Research in partnership with CDW*

However, a seismic shift is underway: Organizations are increasingly involving business line leaders in security policy design and procedural decision-making. More than one-third (35%) of survey respondents say business management, such as the CEO, chairman, president or owner, contributes to security decisions. Other participating business leaders cited among survey respondents include:

- COO, GM, Executive Director, Managing Director — 13%
- CFO, Controller, Treasurer — 13%
- Chief Human Resources Officer — 8%

Surprisingly, a mere 12% of survey respondents say legal counsel is part of a wider team responsible for developing and deploying security policies. A more prominent role for legal team members, and earlier involvement, is essential to helping organizations better prepare for any legal liabilities.

## Conclusion

Organizations must "stay ahead of the security curve by any and all means," declares one survey respondent.

But that takes more than simply deploying powerful prevention tools. Rather, these seven steps can strengthen an organization's risk-mitigation plan without requiring drastic organizational changes or complex technology deployments:

1. Establish a dedicated security function
2. Have a plan for acting quickly — time is of the essence
3. Budget appropriately for security
4. Implement technology that provides better visibility and predictions
5. Engage with trusted third-party partners
6. Implement (and evolve) end-user training — and communicate any changes
7. Extend security responsibilities to business and legal teams

Organizations need not implement these steps overnight. Consolidating the right teams, technologies and risk-mitigation initiatives takes time and experimentation. Flexibility is also key, as security needs (and risks) will evolve over time. However, by scaffolding innovative technologies with cross-functional support and heightened security awareness, organizations can take proactive steps toward minimizing security risks. As one survey respondent puts it, "You can never have enough layers of security."

# ABOUT THE IDG RESEARCH STUDY

To qualify for the December 2017 IDG Research/CDW survey, The Cybersecurity Insight Report, respondents were required to be involved in the purchase process for cybersecurity and/or risk-mitigation solutions and services (see graph, page 23).

Qualified respondents work in an IT-related function at the Manager level or above or a non-IT role at the VP level or above, at a company with 250 or more employees. The average company size was 3,750 employees.

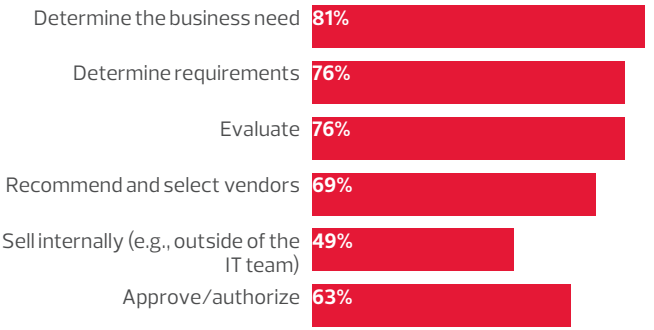
## Respondent Profile — Job Title and Purchasing Responsibilities

### Job Title

| IT-Related (Net) | 54% |
|---|---|
| CIO | 14% |
| CTO | 3% |
| CSO/CISO | 1% |
| Chief Architect | 1% |
| Executive VP/Senior VP/VP | 5% |
| Executive Director/ Managing Director | 5% |
| Director | 15% |
| Manager | 10% |

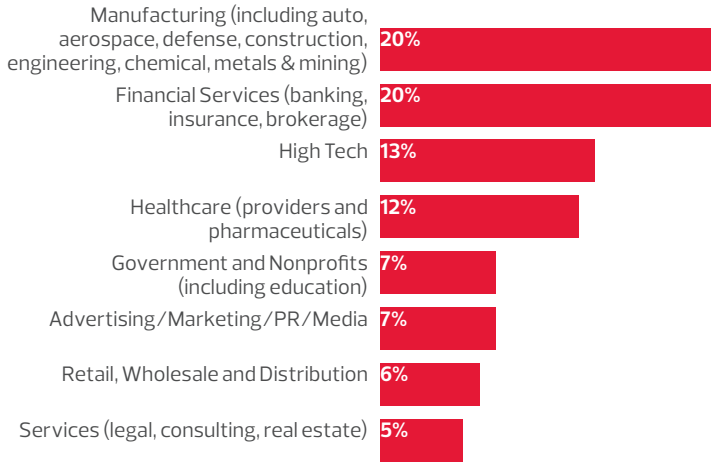
| Non IT-Related (Net) | 46% |
|---|---|
| CEO, COO, Chairman, President | 24% |
| CFO, Treasurer, Controller | 5% |
| Executive VP, Senior VP, VP, General Manager | 17% |

### Involvement in the Purchase of Cybersecurity and/or Risk-Mitigation Solutions and Services



## Respondent Profile – Industry and Company Size

### Top Represented Industries




### Company Size

| | |
|---|---|
| 15,000 or more | 10% |
| 10,000 – 14,999 | 5% |
| 5,000 – 9,999 | 14% |
| 2,500 – 4,999 | 25% |
| 1,000 – 2,499 | 22% |
| 500 – 999 | 13% |
| 250 – 499 | 11% |

**Get an inside look at the next generation of threats and how you can stay prepared at CDW.com/security**


CDW
PEOPLE
WHO
GET IT