THE SECURITY SURVIVAL GUIDE FOR GROWING BUSINESSES

Trustwave®

Smart security on demand

IS YOUR SECURITY GROWING WITH YOUR BUSINESS?

Before we begin, give yourself a pat on the back. By reading this, you're taking an admirable — and often ignored — step toward ensuring the survival of your growing organization.

It's true. Midsize companies tend to place information security in the backseat in favor of fashionable, revenue-generating technical initiatives. Security often gets short shrift because many still-maturing businesses don't view it as a mission-critical component of IT. At best, leaders at these businesses consider security a necessary evil — investing just barely enough to meet industry or regulatory requirements. But the minimal savings gained by that underinvestment in security could end up costing a company millions in regulatory fines and even more in customer revenue and goodwill. If your business is a member of the so-called "mighty middle," it's crucial to know that managing risk is an integral component to capitalizing on the innovation that your IT department drives.

IT has the responsibility not just to expand top-line revenue and create business efficiencies, but also to protect data and prevent breaches in the process. When done well, cybersecurity doesn't have to induce anxiety in technology and line-of-business leaders. It's just a matter of putting in the work and investment.

WANT PROOF THAT BUSINESSES LIKE YOURS ARE UNDER SECURITY DURESS? HERE IS WHAT THE STATISTICS SAY:

LIKELY SCENARIO: In 2015, at least 60% of organizations will discover a breach of sensitive data.[1]

FALSE SENSE OF SECURITY: 70% of businesses believe they're safe from breaches and attacks.[2]

HIGH WATER MARK: A record 1.1 billion personal and sensitive records were compromised in 2014 across 3,014 incidents.[3]

CONTENTS

This guide will walk you step by step through the reasons why your security may be suffering and offer practical tips for addressing your pain points so you can take your data protection to the next level. Don't try to read it all in one sitting — or better yet, hop to the parts that matter most to you and save the rest for later.

SKIP TO THE GOOD STUFF

Remember: While the outlook may look gloomy, there is a lot you can turn to turn things around. The information contained here won't go stale anytime soon, so keep this document close by as you embark on your future security missions. Enjoy!

YOUR BIGGEST CHALLENGES

No company wants to be breached, not even the surprising number that think it can't or won't ever happen to them. A data compromise can mean huge financial and reputational repercussions for an organization of any size. So why, then, are they leaving themselves exposed? Aside from the cultural reasons mentioned earlier — how organizations may look to IT as a revenue booster and consider security a business inhibitor and financial burden — there is a perfect storm of sorts that has settled into the skies above server rooms across the world.

HERE ARE THE BIG 3 IMPEDIMENTS THAT ARE PREVENTING GROWING BUSINESSES FROM ACHIEVING WORRY-FREE SECURITY.

RESOURCE SHORTAGES

IT security budgets, teams and countermeasures can't keep up with the rate at which the number of attackers, threat techniques and vulnerable attack surfaces are increasing.

ADVANCED THREATS

Thanks to a flourishing underground market, sophisticated data-stealing tools, tactics and exploits once available to only well-funded attackers are now finding their way into the hands of a much wider criminal audience.

EXPANDING ATTACK SURFACE

From vulnerabilities in the cloud and Internet of Things to applications and databases, the list of entryways that criminals can use to break into your corporate network has never run longer.

The bad news is that none of these challenges are going away anytime soon. In fact, experts agree that they will actually become much more serious and pronounced over the next several years. The good news, however, is there are actions you can take to minimize the risks that each poses. We'll tell you about those a little later in. For now, let's take a deeper look at all three challenges.

HEY, WHERE IS EVERYBODY?

Many experts argue that the largest security strain facing organizations is their inability to recruit and hire skilled security personnel. This shortage of talent, say security professionals, can be directly blamed for some recent breaches.[4]

The demand for adroit security personnel is far outpacing the supply. Between 2007 and 2013, the number of cybersecurity job postings grew 74 percent, double the growth rate of IT jobs as a whole.[5] Look around at all of the empty space. There is currently an estimated deficit of one million security professionals, a number expected to rise to 1.5 million in roughly five years. Eighty-four percent of IT pros want to increase the size of their security team.[6] And because of this skills gap, salaries for mid-tier cybersecurity professionals are skyrocketing.[7]

There are just not enough qualified people who can keep up with the security demands facing growing and changing businesses. This means that not only can't companies attract human talent, but they are doing themselves no favor by purchasing sophisticated, costly products that will end up collecting dust anyway. Twenty-eight percent of companies own under-deployed security software.[8]

> "IF YOU PUT SOPHISTICATED SECURITY TOOLS IN THE HANDS OF AN UNKNOWLEDGEABLE PERSON WHO HAS NO TIME TO MANAGE THEM TO BEGIN WITH, YOU'RE NOT BEING EFFECTIVE."
>
> – JOHN RAMSEY, TRUSTWAVE

SOPHISTICATED SABOTEURS

The barrier of entry to join the world of cybercrime has never been lower. That's right: No longer do you have to be a veteran hacker or a well-financed or state-sponsored black hat to inflict serious damage on a business.

The cybercriminal marketplace has morphed from a cottage industry into a well-organized machine through which hackers of all skill and experience levels can easily get their hands on sophisticated tools and malware that they can use to snare unsuspecting victims. Underground shops often run just like legitimate businesses — they even offer things like support help and Black Friday deals!

A big reason for this success is exploit kits, which can be used for targeted attacks or to cast a wider net of victims. Exploit kits have become immensely popular in the criminal underground because of their commercial availability and ability to automate the process of infecting large populations of users with advanced malware.

Advanced threats change shape constantly to evade detection, but most of them have similar objectives and behaviors. They generally seek to seize control of a legitimate user account, escalate privileges and probe for and steal valuable data. They attempt to do this through a combination of new exploits, social engineering techniques, phishing, malicious advertisements, password cracking and more.

BREAKING THE BANK

Trustwave SpiderLabs threat researchers determined that attackers can earn a 1,425% ROI through a standard, month-long malware campaign. To calculate the average ROI that can be obtained by the manager of an infection campaign, the researchers accounted for four primary attack ingredients widely available for sale in underground web forums — the payload, infection vector, stolen web traffic and encryption — and then what their cost would be to purchase and use over a month.[9]

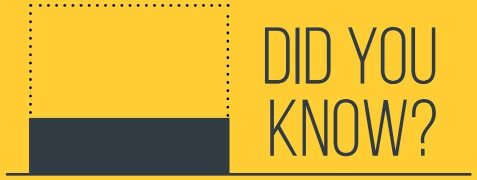
YOUR NETWORK IS LIKE SWISS CHEESE

Technology allows companies to expand, become more efficient and respond to the needs of customers — and the companies that do it best can distance themselves from the competition. But all of this investment comes with a major downside — the possibility that these technologies, infrastructure components and IT delivery models will be vulnerable and invite malicious actions like malware, denial-of-service attacks and sabotage. Never before has the attack surface been so large and vulnerable.

KEY AREAS OF EXPOSURE THAT NEED YOUR ATTENTION

OVERALL SECURITY RISK

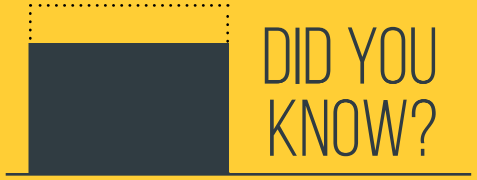
Companies often aren't fully aware of how prone to exposure they are, and have failed to take inventory of all of their sensitive systems and data.



33% of businesses have not commissioned a risk assessment[10]

IT PROJECTS

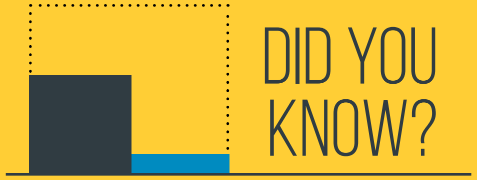
Feeling the need to rush a new app or other technology initiative out the door, organizations often run before they can walk.



77% of IT pros have been pressured to unveil IT projects that weren't security-ready[11]

COMMON SOFTWARE

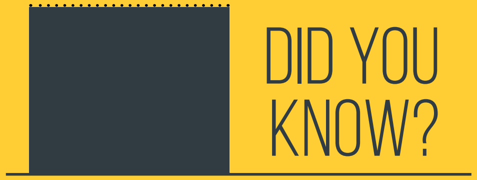
Often advanced malware enters an organization through a vulnerability in commonly deployed software from well-known software makers.



58% of businesses do not have a fully mature patch management process in place, and 12% do not have a patch management process at all![12]

TRADITIONAL ATTACK VECTORS

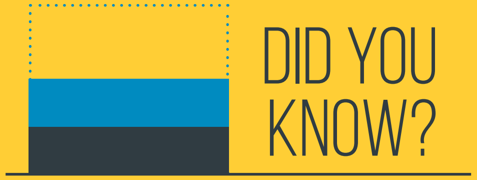
Make no mistake, the customary stuff still works for cybercriminals. Web applications are the front door to your business, and databases are the vault that contains the crown jewels — your sensitive data. Both must be resilient to attack.



98% of web applications tested by Trustwave were found to be vulnerable![13]

WEAK PASSWORDS/ REMOTE ACCESS

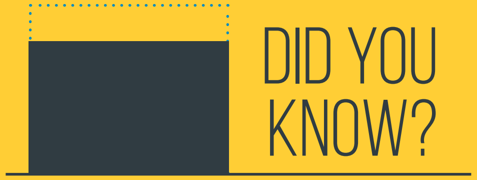
Easily exploitable or default credentials on systems like point-of-sale terminals enable hackers to not only easily penetrate a network, but also propagate once inside.



28% of breaches resulted from weak passwords and another 28% from weak remote access![14]

INTERNET OF THINGS

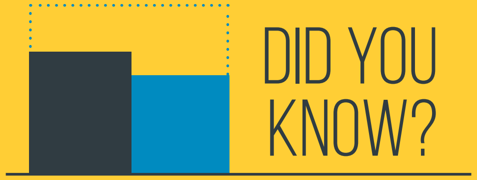
The market for web-enabled technology inside businesses, from point-of-sale terminals to video collaboration robots, is exploding, and organizations are investing billions. Yet if these devices are vulnerable, they can provide a launching pad to the corporate network.



78% of companies are unsure about their capability to secure the Internet of Things.[15]

CLOUD

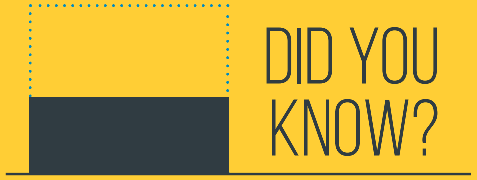
Growing companies tend to be more reliant on cloud services, but compared to larger enterprises, they tend to be less mature around managing adoption and usage.



72% of IT managers don't know the number of "shadow" applications being used in their organization, and 57% receive between one and 10 new cloud service requests each month.[16]

INSIDER THREATS

Whether malicious or not, insiders with legitimate access to network resources can put business assets at risk. Clueless employees can make it easier for attackers by clicking on malicious links and falling for phishing scams. Meanwhile, unmonitored insiders can leverage their access to commit fraud.



45% of companies couldn't tell if they'd experienced an insider attack in the last year.[17]

WHY GROWING BUSINESSES ARE A PRIME TARGET

IT CAN HAPPEN TO YOU

It's easy for midsize businesses to fall into the "it won't happen to me!" trap when it comes to cybersecurity. From IT leadership, all the way up to the top of the C-suite, management at these firms wants to dedicate as much of its slim technology resources as possible to support innovation and revenue growth. On the flip side, cybersecurity often looks like a cost center.

Part of the blame belongs to poor communication of cyber risk information to executive leaders and other decision-makers that control the coffers. But the No. 1 objection that midsize businesses make about increasing security spending is that if it ain't broke, don't fix it. If we haven't been breached yet, we must be doing something right…right?

Sorry, no.

Barring some ridiculous luck, something is almost definitely broken, but the trouble is that most expanding businesses don't have the resources to see it. Many IT leaders and others at midsize firms take the absence of detection as a sign that they're not being actively targeted. But the bad guys today have gotten incredibly good at being sneaky and successful.

Growing businesses generally aren't even investing enough in the technology to detect the most dangerous attacks, let alone protect against and respond to them. Consider this: from 2013 to 2014, breaches of small to midsize enterprises rose 64 percent.[18]

YOU'VE ALREADY BEEN BREACHED

There's a popular saying in the security industry. There are two types of companies — ones that have been breached and ones that don't know it yet. In fact, growing businesses that don't ever find much evidence of security incidents in their IT infrastructure should probably be the ones most worried about their state of security readiness. Most security experts today agree that companies should operate under the assumption that they've already been compromised. Attackers are so stealthy and proficient at what they do, the likelihood is high that they've staked their ground on some endpoint or server somewhere, if not completely owned your network, without anyone noticing.

This means that if you aren't finding these breaches, the attackers are probably just too good for you to notice their presence.

TRY THESE STATS ON FOR SIZE:

Last year, more than four out of five organizations needed outside help to detect breaches.[19]

The average time between initial intrusion to detection is now 188 days — more than six months.[19]

Some compromises have allowed attackers to infiltrate systems for more than four years at a time.[19]

Now consider that these stats are an average for ALL organizations, including large enterprises with huge IT budgets. Midsize performance in these areas would be expected to suffer even more due to the major challenges already addressed in this guide.

"EVERY COMPANY WILL BE COMPROMISED SOONER OR LATER. NO ORGANIZATION IS IMMUNE."

-JAKE WILLIAMS, SANS INSTITUTE[20]

"ATTACKERS TARGET COMPANIES OF ALL SIZES. NO MATTER HOW OBSCURE YOU THINK YOU MAY BE, YOU SHOULD EXPECT TO BE EVENTUALLY ATTACKED."

-ERIC COLE, SANS INSTITUTE[21]

Attackers have the choice among some 70 different exploit kits on the black market today[22]

The FBI reports that cybercriminals have made more than $18 million from a single piece of malware alone. Called CryptoWall, it's ransomware that breaks into the victim's system and encrypts data to hold it hostage until the victim pays attackers off.[25]

WHY ATTACKS RUN RAMPANT

So how is it that attackers are eventually able to run roughshod over just about any organization's systems? Earlier we got into the general drivers for the dismal state of affairs. Now let's dig a little deeper.

UNFAIR ATTACK ADVANTAGE: Defenders must be able to stop every single type of attack to prevent a compromise on their systems, whereas attackers only need to be right once to get their foot in the door. The bad guys know this, which is why they put their shoulders into throwing a large volume and variety of attacks against businesses, with the expectation that eventually one of them will work. Even targeted attacks are repeatedly tried against a single subject to ensure that a well-crafted spear phishing email eventually hits its mark.

Attackers unleash nearly one million new malware variants of malware online every day[23]

AUTOMATED ATTACKS: Adversaries are able to scale up a huge number of new attacks against a wide range of targets because they're arming themselves with an arsenal of easy-to-use tools. Hacker toolkits like Magnitude and RIG automate a malware attack like something off an assembly line in a factory. For example, they seek out online systems with common vulnerabilities and then spam out millions of malicious phishing message to steal valuable sensitive data.

Just a single exploit kit, used in a single attack campaign, infected 1.25 million victims in six weeks[24]

ATTACKERS ARE MAKING MONEY: The cybercrime world is all about the bling. These days, attacks feed a rapidly growing, illegal business empire that makes money off of stolen credit cards, accounts, medical records and even corporate intellectual property. Attackers are willing to invest in exploit kits, new malware variants and other attack tools because they know they'll earn huge returns on their investment.

THE PATH OF LEAST RESISTANCE

Since cybercrime syndicates are essentially business entities, their primary purpose in life is to find the path of least resistance for making the biggest profit possible. And, let's face it, in the world of security, growing organizations usually sit squarely on that path. Midsize businesses are a gold mine for cybercrooks because they tend to deal in a higher volume of sensitive data than their smaller counterparts, yet still have far more immature data protection mechanisms than the larger enterprise.

Even if attackers can't make as much profit off a single midsize entity as they can from a larger enterprise, they can make up for the difference by going after multiple victims, enabled by their ability to automate attacks.

SECURITY MISPERCEPTIONS ARE COSTLY

Two-thirds of small and midsize enterprises don't consider their business to be vulnerable[26]

Just 16% say they're making cybersecurity improvements a priority in 2015[27]

They put one-third of their revenue at risk through poor security practices[28]

The average cost of a breach in security has doubled since 2013[29]

More than 80% have suffered downtime in the past 12 months as a result of security incidents[30]

WHAT MAKES YOUR BUSINESS AN EASY MARK?

THERE ARE THREE BIG REASONS MID-TIER ORGANIZATIONS ARE HUNTED DOWN BY THE BAD GUYS

BECAUSE YOU PARTNER WITH A BIGGER TARGET

Growing organizations are often the weakest link in an ecosystem of businesses partnering with each other. Many intrusions are springboards for attacks against a larger company. The bad guys will target a smaller enterprise with the understanding that this little fish can be used to catch a lunker later on down the line. Large enterprises tend to have bigger security budgets and tougher defenses to crack. An attacker seeking a bulkier target will often find it much easier to first go after a midsize business that provides contract labor to that enterprise, such as business consulting, billing services or temp staffing. It is then just a matter of exploiting trusted digital connections between the compromised company and the larger target — and, voila, criminals claim their prize.

BECAUSE YOU HOUSE JUICY DATA

Midsize businesses have plenty of their own juicy data in-house, too. Many of these outfits operate in specialized verticals that often deal in boatloads of sensitive information and customer records. In many instances, growing companies have more to lose on the intellectual property front, as these businesses usually innovate at a faster clip than their larger counterparts and depend heavily on IP for their market advantages. Believe it or not, thefts like these occur every day, even if they aren't in the news like big customer data breaches. Companies tend not to report IP theft because they aren't legally required to do so.

BECAUSE YOU'RE A SOFT TARGET

Automation of hacking tools makes it trivial and cheap for bad guys to trawl the internet for weak targets and use the opportunity to scoop up information and systems that could be sold or used later. This could be stolen credit card data that could be sold to cloners to create counterfeits, intellectual property that could be sold to interested parties wanting to gain a competitive advantage, or simply control over computers that help attackers carry out future intrusions.

Opportunistic attackers will look for public facing web servers with applications vulnerable to common exploits, such as SQL injection. They can do this through automated search engine queries and by scanning network block ranges looking for vulnerable web servers. Once they find a web app or server that might be exploitable, they'll do one or more of the following:

Install hidden backdoors on the system to get a foothold for more exploration into the network

Install software to control the system and recruit it to belong in a botnet that can be used to spam other victims or carry out distributed denial-of-service (DDoS) attacks

Install drive-by-download malware that can be served up to future visitors of the websites and silently infect those visitors' computers through their web browser

All options are profitable for the attacker.

97% of people can't correctly identify phishing emails[31]

TOP 5 WAYS ATTACKERS COMPROMISE GROWING BUSINESSES

1. PHISHING

Phishing attacks are one of the most common and longest-lived attack techniques that cybercriminals use to break into systems. In its simplest form, a phishing attack is pulled off when crooks spam out a mass mailing of emails to potential victims, posing as institutions that people commonly deal with, like banks, shipping services, online retailers and so on. The idea is to send recipients to a spoofed site in order to trick them into divulging sensitive information, such as login credentials.

Phishing Progresses

From human's earliest days, social engineering has been a tried-and-true way to con people. Fast forward a couple of hundred thousand years to the digital era, and attackers are constantly evolving techniques based on this age-old approach to become more effective and profitable.

For example, bad guys may still send out a mass email, but rather than initially seek login information, the goal is to get a recipient to open a malicious attachment that contains malware that will infect the victim's machine. This malware might consist of multiple parts, including password stealers that will be able to rip off not just one but every password used by the victim on that machine, including corporate credentials. Or the malware could be ransomware, a growingly popular threat that encrypts computer files on PCs and mobile devices — and then demands a payment from victims to unlock their data.

Similarly, attackers also use phishing emails to trick users into simply visiting a website infected with malware that will quietly load itself onto their machines without their knowledge in what's known as a drive-by download. In these cases, it doesn't require more than a click to work.

PHISHING CONTINUED

Spear Phishing

Attackers also engage in spear phishing attacks, which target very specific victims, such as a company leader or senior executive. The criminals behind them typically have the luxury of resources, time and determination on their side. As such, these attacks are more elaborate and costly for the bad guys, but if they succeed, the rewards are more lucrative — for example, full compromise of a business executive's machine, which might have the highest level of access to corporate systems and data.

An attacker usually starts by conducting reconnaissance about a targeted victim. For example, the attacker might learn from social media about that person's hobbies and then craft a convincing email to bait the victim into clicking a link or opening an attachment. The malware in question is likely to also be more advanced than standard phishing malware, sometimes exploiting previously unknown 'zero-day' vulnerabilities on the victim's system.

Taking the Bait: Common Phishing Lures

Some of the most common 'bait' that phishing attacks use to convince users to open up attachments, click links or provide login information include fake:

- Invoice notices
- ACH transfer notices
- Breaking news alerts
- Package delivery and order confirmations
- Job board alerts
- Security alerts
- PowerPoint attachments

Be especially wary if you receive emails like this — and only open and interact with them if you were expecting them. Spread this same advice to your employees.

5 WAYS CONTINUED

2. UNPATCHED SYSTEMS

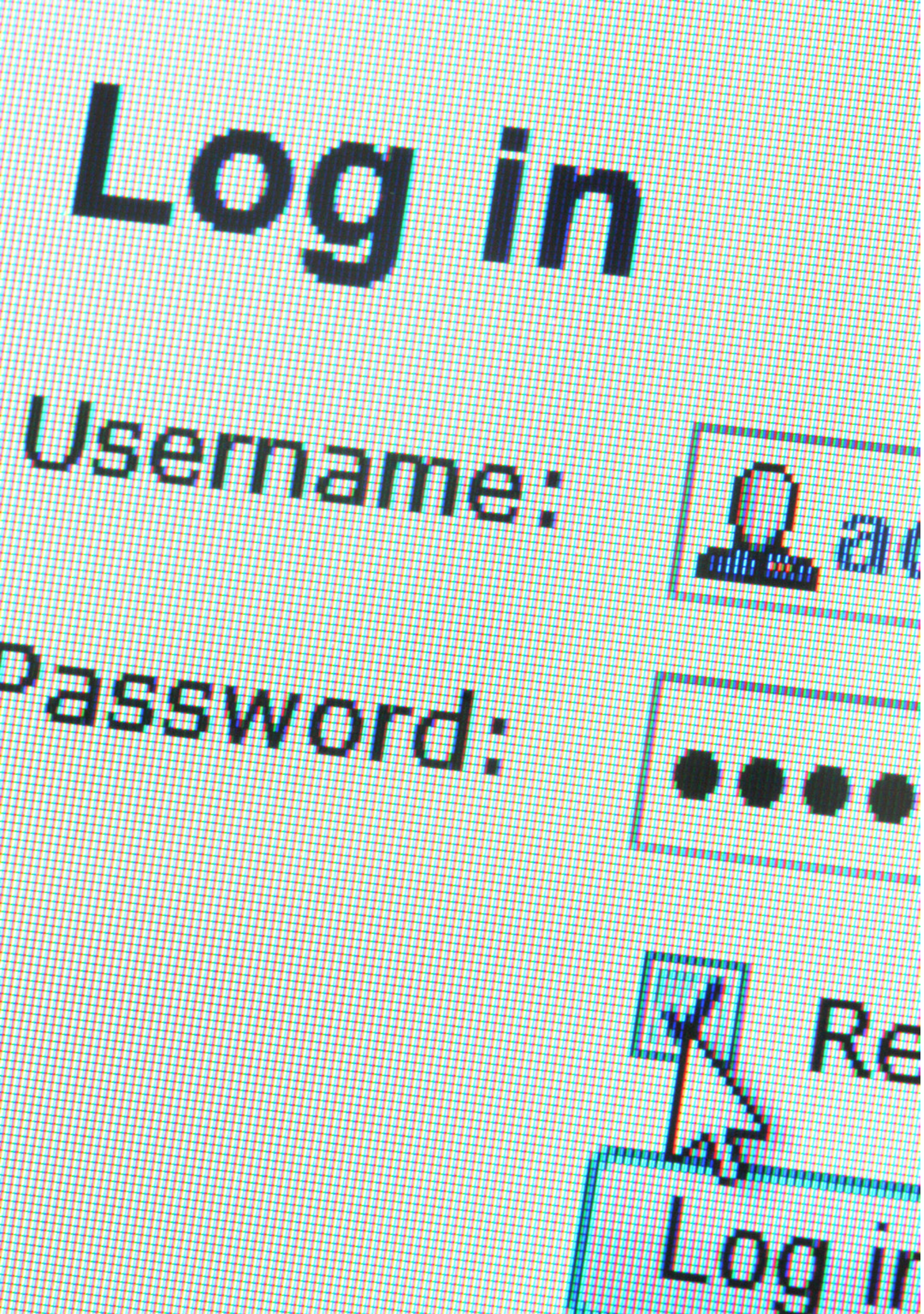
Ninety-seven percent of the attacks carried out in 2014 exploited just 10 known vulnerabilities in common software, such as Microsoft Office applications, Adobe Reader, Adobe Flash and Java.[32] These were vulnerabilities for which vendors had provided software updates to fix, but victims failed to apply the patches. Known vulnerabilities are the low-hanging fruit, but this attack statistic shows that many organizations leave them on the tree, unpatched.

3. MALWARE EXPLOIT KITS

Malware toolkits are software packages that automate the entire process of compromising victims, from soup to nuts, including

- Identifying and exploiting vulnerabilities in a victim's computer
- Providing a centralized command-and-control hub to manage a large number of compromised machines
- Delivering malware payloads onto the target machine
- Providing evasion mechanisms to keep the kit from being detected by typical anti-malware technology
- Creating a backdoor system for the attacker to control the compromised machine

Exploit kits can be purchased on a subscription lease basis from black market developers for as little as $150 per week. They're often paired with phishing techniques to create a comprehensive attack campaign.[33]



4. DEFAULT OR WEAK PASSWORDS

Users are notorious for skimping on their passwords. Most penetration testers find that default or weak passwords, such as 'Password1,' are rampant in growing businesses and account for some of the most dangerous vulnerabilities in application and network environments, including remote access software.

In one study of close to a half-million encrypted passwords, security penetration testers from Trustwave were able to crack 51 percent of them within 24 hours and 88 percent within two weeks.[34] Trustwave researchers found that a password with eight characters can be cracked in just one day using brute-force attack techniques.[35] In many instances, brute-force attacks aren't even necessary, as users tend to pick easy-to-guess passwords or just use default passwords from their systems.

5. LATERAL MOVEMENT

When users fail to protect important systems and network connections with strong passwords, they give attackers who have a foothold on one system an easy opportunity to make their way laterally across the network to compromise many more systems. This is a typical modus operandi for attackers, who regularly turn a simple compromise of an endpoint or a web server into a full-scale assault of assets across the network. Account takeovers are made possible when organizations fail to enact network access control and monitoring of network activity to watch for attackers moving and compromising network resources for extended periods of time.

TOP 10 PASSWORDS

The following are the top 10 most popular passwords in a study of 499,556 passwords conducted by Trustwave security researchers.

PASSWORD	COUNT
Password1	4,585
Welcome1	3,690
P@ssword	3,120
Summer1!	1,960
password	1,694
Fa$hion1	1,313
Hello123	1,196
Welcome123	1,143
123456q@	1,078
P@ssword1	921

8 PRO TIPS FOR STRONGER PASSWORDS

ADD COMPLEXITY

The time it takes to crack to crack an eight-character password and a 10-character password is the difference between one day and hundreds of days.

USE PASSPHRASES

Believe it or not, an easy-to-remember phrase (such as "GoodLuckGuessingThisPassword") is actually stronger than a random string of special characters.

CHANGE PASSWORDS FREQUENTLY

Passwords should be changed every 60 to 90 days, depending on whether the sensitivity of the account is generic or elevated privilege. And don't forget to avoid using the same password across multiple accounts.

SALT AND HASH

While the combination sounds like something you might do in the kitchen, IT administrators should use unique, random "salts" when "hashing" stored passwords, whereby a piece of unique, random data is combined with each password before the hash is calculated.

IMPLEMENT STRONG PASSWORD POLICIES

Password complexity policies, particularly in Windows, don't take into account the context of a password, such as identifiers from the company, a company product, the city in which the company operates or the local sports team.

AUDIT PASSWORDS

Companies need to perform password audits to find the weak links. Often times, the weakest link are the non-tech-savvy users, who are considered soft targets by attackers.

IMPLEMENT A PASSWORD MANAGEMENT SYSTEM

Password managers encrypt, store and fill out your passwords for all the sites you use - and you only need to remember the master password to unlock them all.

CONSIDER TWO-FACTOR AUTHENTICATION

This technology supplements passwords by providing a second form of verification. Thus, if a user's password is compromised, the second-factor, such as a token or a code sent to your phone, acts as another layer of defense.

COVERING THE BASICS

WHERE DO GROWING BUSINESSES GO WRONG?

Regardless of why mid-level businesses are targeted, they are prone to security lapses for a wide range of reasons.

TECH RISK TAKING: First of all, many of these organizations are more likely than their larger counterparts to innovate using technology or digital collaboration tools with unproven security. This kind of technology experimentation can prove profitable for organizations but dramatically increases the risk to the organization. Risky technology initiatives include bring-your-own-device (BYOD) programs, unrestricted use of apps, cloud collaboration and file sharing, and Internet of Things devices connected to corporate networks and machines.

STODGY SECURITY TECHNOLOGY: Even though they're quick to jump on just about any new cutting-edge general business technology that can improve productivity, expanding organizations often stick with one or two mainstay security technologies that they've been automatically subscribing to for years. While anti-virus and firewalls remain important technologies for protecting against a large volume of basic attacks, relying solely on these tools puts these businesses at risk.

WIDE DISTRIBUTION OF OFFICES: Whether they're retail or hospitality outfits with numerous stores or growing businesses with expanding branch offices scattered across large regions, midsize organizations tend to be highly distributed. Unlike larger enterprises with big budgets, they may not have the resources to hire an adequate number of IT or security staffers beyond those team members hunkered down at headquarters.

WHERE DO GROWING BUSINESSES GO WRONG, CONT'D.

UNTRAINED AND UNMONITORED INSIDERS: Insiders granted access to sensitive data can inflict some serious hurt on growing businesses if they have little knowledge of important security principles and their usage is not monitored. Negligent insiders can make it exponentially easier for attackers to gain unauthorized access to their accounts by falling for phishing scams and visiting infected sites. And malicious insiders — the ones who are purposely up to no good — can use their legitimate credentials for nefarious purposes without any consequences if businesses don't monitor their activity.

5 TYPES OF DANGEROUS INSIDERS

THE ABSENT-MINDED is a worker who unwittingly places the company at risk due to poor security practices.

THE REVENGE SEEKER is a malcontent who acts out by destroying sensitive data or stealing it, perhaps to be used at their next job.

THE PRIVILEGE ABUSER is someone who has gained access to more assets than necessary to do their job and isn't afraid to snoop.

THE PARTNER is a contractor or other non-employee who might not be protecting their network credentials from being hacked.

THE COLLUDER is someone who works with an external party to divulge credentials in order to perpetrate a data breach.

POOR SECURITY BUDGET ECONOMIES OF SCALE: As we've mentioned, targeted attackers often have big budgets when choosing their weapons, and it takes numerous layers of security technology and a knowledgeable staff to effectively analyze and respond to threats using those layers (check out page 24 for more details on this). In the end, the issue is one of economies of scale. Mid-level organizations simply do not have the resources in house to address the entire threat landscape today. There are simply too many moving parts for the average company to establish enterprise-class security on the budget of a smaller organization.

INDIVIDUAL INDUSTRY CHALLENGES

Depending on your industry, you'll face different security impediments and priorities. Understanding what makes each vertical market unique will help you better confront threats. But one important thing to remember is that all industries are under attack, and cybercriminals are moving their attacks down the business food chain — and mid-tier companies are right in their cross-hairs.

We've broken down the security attributes of each industry, and you may notice that compliance is largely missing. That's on purpose. While many sectors have specific requirements governing them, the fact is compliance is the ground floor for security. Those businesses that implement advanced, comprehensive and continuous security are much closer to having the checkboxes covered rather than those that just focus on a specific rule or regulation.

FINANCIAL SERVICES

These firms, including banks and brokerage houses, are in the sights of a range of attackers, from state-sponsored adversaries after trade secrets and intellectual property, to financially motivated crooks interested in sensitive client data, to politically motivated hacktivists seeking to cause disruption through things like DDoS attacks. While these organizations are typically more advanced in their security controls than other industries, experts believe they could be doing much more considering how high value of a target they are. Many are responding by boosting spending.

HEALTH CARE

Online health records, cloud services and the Internet of Things are providing ample motivation and vectors for both external attacks and insider theft. Meanwhile, the value of stolen patient records — which enables medical identity theft and insurance fraud — has soared in the criminal underground, fetching up to 50 times as much as stolen credit card numbers.[36]

GOVERNMENT

One of the hardest-hit industries, government agencies are big targets because they are the largest holder of data in the world. The number of security incidents against these organizations in the United States has increased 12-fold since 2006, and a big reason why is agencies simply aren't spending enough. [37]

INDIVIDUAL INDUSTRY CHALLENGES, CONT'D.

> "SEVERAL YEARS AGO, A LOCAL TELCO HIRED A SYSTEM INTEGRATOR TO GO RIGHT UP AND DOWN 'RESTAURANT ROW' IN A SMALL TOWN TO CONVERT EVERYBODY OVER TO BRAND-NEW POINT-OF-SALE (POS) SYSTEMS. THEY PUT THESE SYSTEMS ON THE INTERNET WITH NO FIREWALLS, AND THE SYSTEM INTEGRATOR BASICALLY JUST MADE A CARBON COPY OF THE POS FOR EVERY ONE OF THESE LOCATIONS. ONCE THE BAD GUYS FOUND ONE, THEY JUST WALKED THAT IP RANGE THAT BELONGED TO THAT ISP. WE HAD — IN THIS LITTLE TINY TOWN IN THE MIDDLE OF AMERICA — ABOUT SIX OR SEVEN LOCATIONS GET BREACHED WITHIN TWO WEEKS OF EACH OTHER. OVER HALF OF THEM HAD TO CLOSE THEIR DOORS BECAUSE THEY COULDN'T EVEN AFFORD THE FORENSIC INVESTIGATIONS."
>
> – DON BROOKS, TRUSTWAVE

EDUCATION

Remember we talked about that path of least resistance? Well, at colleges and universities, intruders typically find a much more appealing road than they would at a typical enterprise. This is due to the transient and remote end-user base — which can introduce risks, such as malware, each time they reconnect to the campus network — and the openness and decentralized culture of these institutions.

MANUFACTURING

As digital connectivity grows, these businesses have come under increased scrutiny due to the increasing likelihood of vulnerabilities popping up somewhere in the supply chain. In addition, vulnerable IoT technologies — such as "smart" sensors placed on an assembly line to improve efficiency — can place manufacturers in harm's way. At most risk for theft are precious intellectual property and trade secrets.

RETAIL/HOSPITALITY

The source of some of the most high-profile data breaches in recent years, these businesses face attacks due to the huge amount of payment card numbers they process. Franchise organizations, which have multiple sites, often suffer from similar vulnerabilities and make for easy pickings. And while card breaches — mostly related to e-commerce and point-of-sale systems — are the most widely publicized intrusions, criminals are also focusing on back-office systems, such as payroll and HR.

SO, WHERE TO BEGIN?

Businesses that truly want to develop effective security programs have to start somewhere. The logical first step is to take a look in the mirror and conduct an honest review of where your organization's security posture stands.

This means conducting a full-fledged risk assessment that includes the following:

- **Where data lives within the enterprise and how it moves, both internally and outside the organization**
- **Inventorying systems to understand their patch and vulnerability status**
- **Evaluating applications for vulnerabilities**
- **Understanding current volumes of detected security incidents and how long it takes to respond to these known incidents**

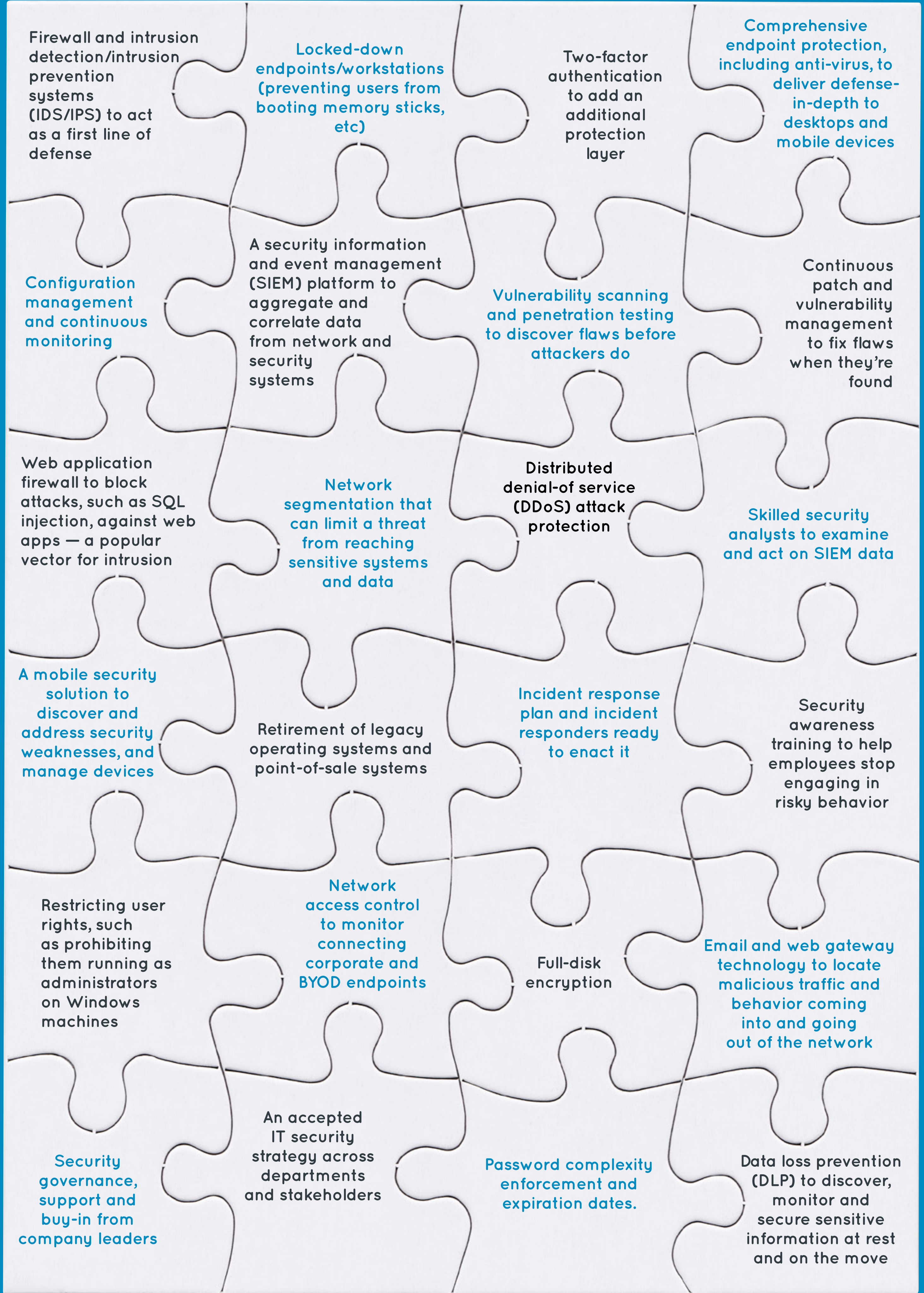
Additionally, a business trying to expand and evolve its security must consider a couple of important management tasks. First, an organization must be able to strongly vet and ensure the security of third-party partners before contracting with them, and continue doing so throughout its relationship with them.

And second, technology leaders need to be able to communicate risk clearly to business leaders by speaking in digestible, non-technical terms that they can understand. This collaboration involves a variety of internal and external stakeholders:

o C-Suite and board
o Regulators
o Franchisors
o Clients
o Consumers
o Business partners

PIECE TOGETHER YOUR SECURITY PUZZLE

Security is hardly a monolithic entity. It requires a solid mix of experienced people, well-thought-out processes and up-to-date technology to succeed. The following components are the major pieces that every maturing business should at least consider to properly manage risks — emanating from not only the outside, but also the inside.



Firewall and intrusion detection/intrusion prevention systems (IDS/IPS) to act as a first line of defense

Locked-down endpoints/workstations (preventing users from booting memory sticks, etc)

Two-factor authentication to add an additional protection layer

Comprehensive endpoint protection, including anti-virus, to deliver defense-in-depth to desktops and mobile devices

Configuration management and continuous monitoring

A security information and event management (SIEM) platform to aggregate and correlate data from network and security systems

Vulnerability scanning and penetration testing to discover flaws before attackers do

Continuous patch and vulnerability management to fix flaws when they're found

Web application firewall to block attacks, such as SQL injection, against web apps — a popular vector for intrusion

Network segmentation that can limit a threat from reaching sensitive systems and data

Distributed denial-of service (DDoS) attack protection

Skilled security analysts to examine and act on SIEM data

A mobile security solution to discover and address security weaknesses, and manage devices

Retirement of legacy operating systems and point-of-sale systems

Incident response plan and incident responders ready to enact it

Security awareness training to help employees stop engaging in risky behavior

Restricting user rights, such as prohibiting them running as administrators on Windows machines

Network access control to monitor connecting corporate and BYOD endpoints

Full-disk encryption

Email and web gateway technology to locate malicious traffic and behavior coming into and going out of the network

Security governance, support and buy-in from company leaders

An accepted IT security strategy across departments and stakeholders

Password complexity enforcement and expiration dates.

Data loss prevention (DLP) to discover, monitor and secure sensitive information at rest and on the move

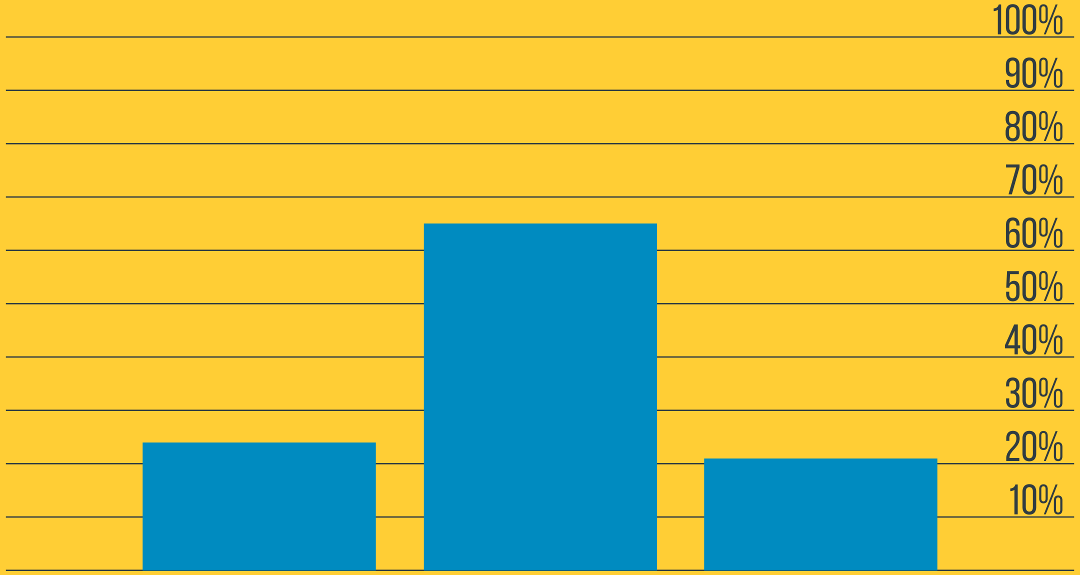
START AN EDUCATION REVOLUTION

As important as all of these puzzle pieces are to improving your security IQ, perhaps the most rewarding investment a growing business can make is in strengthening security's weakest link: clueless employees.

As we've mentioned before, by engaging in sloppy security behavior, negligent insiders make it much easier for attackers to break through defenses. And yet, many businesses today do little to train these employees on the various situations they may encounter.

Employees, if properly trained, can provide a valuable frontline defense for any size organization. Implementing a regular awareness and training program covering both policy and procedures is an easy and beneficial first step toward security success.

A GUIDANCE GAP



24% of businesses don't have employees read and sign an information security policy.[38]

65% of business don't train employees on security more than once a year.[38]

21% of businesses never perform security awareness training.[38]

TIPS FOR EFFECTIVE SECURITY AWARENESS TRAINING

MAKE IT INTERACTIVE

Students retain information that is presented interactively at 3x-10x the rate of information presented through static methods.[39]

MAKE IT REPETITIVE

Annual retention rates can be doubled when companies provide smaller refresher courses that are given on a monthly or quarterly, rather than annual, basis.[40]

TELL STORIES

Connect theoretical teachings with real life by explaining it through stories and anecdotes with which workers can relate.

MAKE IT ACTIONABLE

Give employees day-to-day tips on how to put their knowledge to work.

PROVIDE INCENTIVES

You should not only make employees feel comfortable reporting a mistake they made, but you can also reward good behavior. One idea is to do that through gamification.

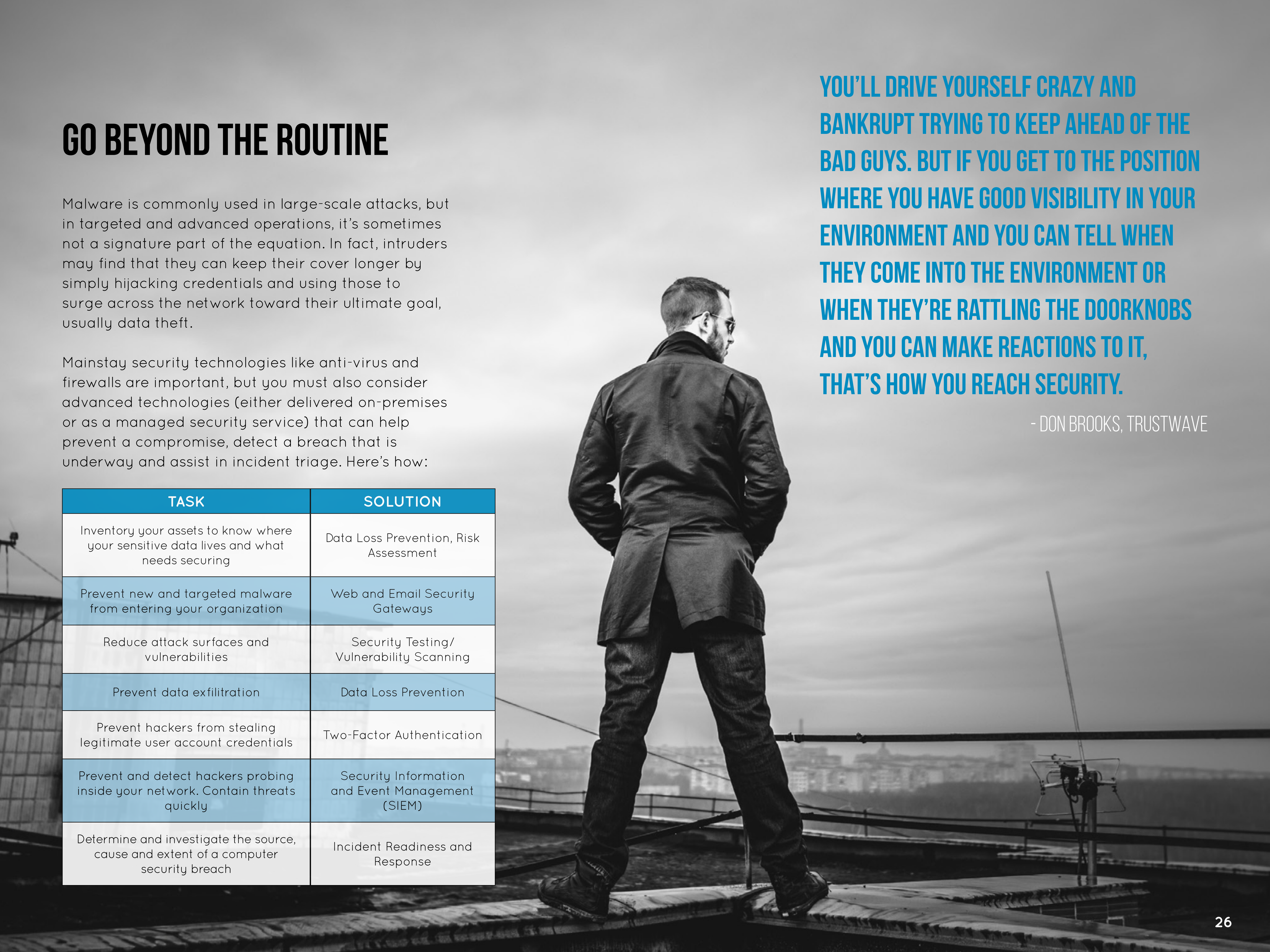
GO BEYOND THE ROUTINE

Malware is commonly used in large-scale attacks, but in targeted and advanced operations, it's sometimes not a signature part of the equation. In fact, intruders may find that they can keep their cover longer by simply hijacking credentials and using those to surge across the network toward their ultimate goal, usually data theft.

Mainstay security technologies like anti-virus and firewalls are important, but you must also consider advanced technologies (either delivered on-premises or as a managed security service) that can help prevent a compromise, detect a breach that is underway and assist in incident triage. Here's how:

TASK	SOLUTION
Inventory your assets to know where your sensitive data lives and what needs securing	Data Loss Prevention, Risk Assessment
Prevent new and targeted malware from entering your organization	Web and Email Security Gateways
Reduce attack surfaces and vulnerabilities	Security Testing/ Vulnerability Scanning
Prevent data exfiltration	Data Loss Prevention
Prevent hackers from stealing legitimate user account credentials	Two-Factor Authentication
Prevent and detect hackers probing inside your network. Contain threats quickly	Security Information and Event Management (SIEM)
Determine and investigate the source, cause and extent of a computer security breach	Incident Readiness and Response

> YOU'LL DRIVE YOURSELF CRAZY AND BANKRUPT TRYING TO KEEP AHEAD OF THE BAD GUYS. BUT IF YOU GET TO THE POSITION WHERE YOU HAVE GOOD VISIBILITY IN YOUR ENVIRONMENT AND YOU CAN TELL WHEN THEY COME INTO THE ENVIRONMENT OR WHEN THEY'RE RATTLING THE DOORKNOBS AND YOU CAN MAKE REACTIONS TO IT, THAT'S HOW YOU REACH SECURITY.
>
> - DON BROOKS, TRUSTWAVE



THE FUTURE IS HERE:
MOBILITY AND INTERNET OF THINGS

No matter the size of your company, bring-your-own-device (BYOD) and the Internet of Things have turned into full-fledged business tools. But amid all of the productivity and customer engagement wins that can come from them, organizations must start and end their strategies with security. What can you do?

TEST

Before deploying, you must identify vulnerabilities, reduce threats and strengthen the security of your mobile and IoT deployments across your entire ecosystem, as well as ensure the resilience and performance of your mobile apps and platforms. Test, don't guess!

PROTECT

Whether you are deploying a mobile point-of-sale device, the hottest new application or a web-enabled machine component, ensuring that these endpoints can't be compromised is paramount. Security solutions should provide visibility, as well as defense against fraud, tampering and infiltration.

EDUCATE

Empower your employees with the security know-how to help protect your business against growing security risks and compliance missteps.

TAKE A LOOK IN THE MIRROR

Clearly, security is a problem that requires many moving pieces to solve. But in all likelihood, the plurality of threats has grown to the point where you can't feasibly understand and react to them all. As this guide has shown, the only way a growing business can mitigate all the threats it faces is to invest in layered solutions and experienced staff to help run them.

ASK YOURSELF:

1. **Are you 100 percent confident your current technology can spot stealthy attacks?**

2. **Is your business capable of investing the level of technology resources this guide outlines to establish a solid security foundation?**

3. **Can your in-house staff deploy and manage all of these layers of security technology and act on the intelligence they provide — even if they fear being blamed for an incident?**

4. **Do you have the resources to quickly respond to security incidents?**

5. **Does maintaining robust security make sense for the scale of your business?**

If you answered 'no' to most or all of these questions, you might want to reconsider your existing security strategy.

THE CASE FOR MANAGED SECURITY SERVICES

CHECK OUT THIS SPECIAL REPORT "WHY MOVE TO AN MSSP: SECURING I.T. IN AN ERA OF THREAT SURPLUS AND TALENT SCARCITY" ➦

This is where managed security services come in. Managed security provides the opportunity to leverage enterprise-class solutions without having to build out the infrastructure or staff to support them. In many instances, managed security service providers (MSSPs) actually deliver better security for customers than even advanced large enterprise can for themselves due to the economies of scale and threat intelligence they gather by serving many organizations at once.

Best of all, the financial justification for MSSP-delivered security is usually superior to in-house security. Rather than racking up capital expenditures that will inevitably grow obsolete, businesses can put the tab in the operational expense column and rely on its service provider to make necessary upgrades without ever having to endure large unforeseen cash outlays when those upgrades need to happen.

78% of IT and security professionals already partner or are likely to partner with a managed security services (MSS) provider to relieve their infosec pressures.[41]

EVALUATE YOUR MSSP

QUESTIONS TO ASK YOUR POTENTIAL PROVIDER

How big is the provider's security operations center team and do its SOCs operate in a follow-the-sun model, 24x7?

Does the provider have an in-house security research group?

Does the provider develop its own security technology to support its operations or does it rely solely on other vendors?

How experienced is its incident response staff and how quickly can it help your firm investigate and respond to security events?

How well does the provider partner with other vendors to create a best-of-breed layering of security technologies?

FIND YOUR SECURITY SOUL MATE

In the end, it doesn't seem sustainable or feasible to deal on your own with all of challenges this guide has addressed. So you have to ask yourself: Is do-it-yourself viable in the context of today's threat? Perhaps it is, but more likely it's not — at least for all of your security. A managed security services provider can step in and handle the burden so you can concentrate on revenue-generating IT projects.

A DUE DILIGENCE CHECKLIST FOR PARTNERING WITH AN MSSP

EXPERTISE

Delegating some of the work to a trusted partner whose staff includes highly skilled and renowned security and compliance experts, ethical hackers, researchers and incident responders is an easy way to bridge the talent gap.

ADVANCED SECURITY

Even novice attackers now have access to advanced malware, which is why you should look to managed providers that offer high-value security solutions, such as anti-malware, SIEM and security/vulnerability testing.

THREAT INTELLIGENCE

The bad guys never sleep, and neither does your business. Look to MSSPs that offer round-the-clock coverage that follows the threats, and can help ensure security events and incidents are immediately discovered and dealt with — before they can cause big damage.

CUSTOMER SERVICE

No business is the same, and you should search for MSSPs that — at the outset of the relationship — recognize that they must customize their offering based around your organization's individual needs. And, if problems do arise, responsiveness, communication and speed should be defining characteristics of the provider.

For more help on boosting your security
or to talk to an an expert, visit
www.trustwave.com/services

Trustwave®
Smart security on demand