AT&T Business

AT&T Cybersecurity

SHIELDS down

1 in 2 IT pros admit cybersecurity policies are ad hoc, not integrated

ALIEN LABS

CYBERSECURITY INSIGHTS VOL. 8.5

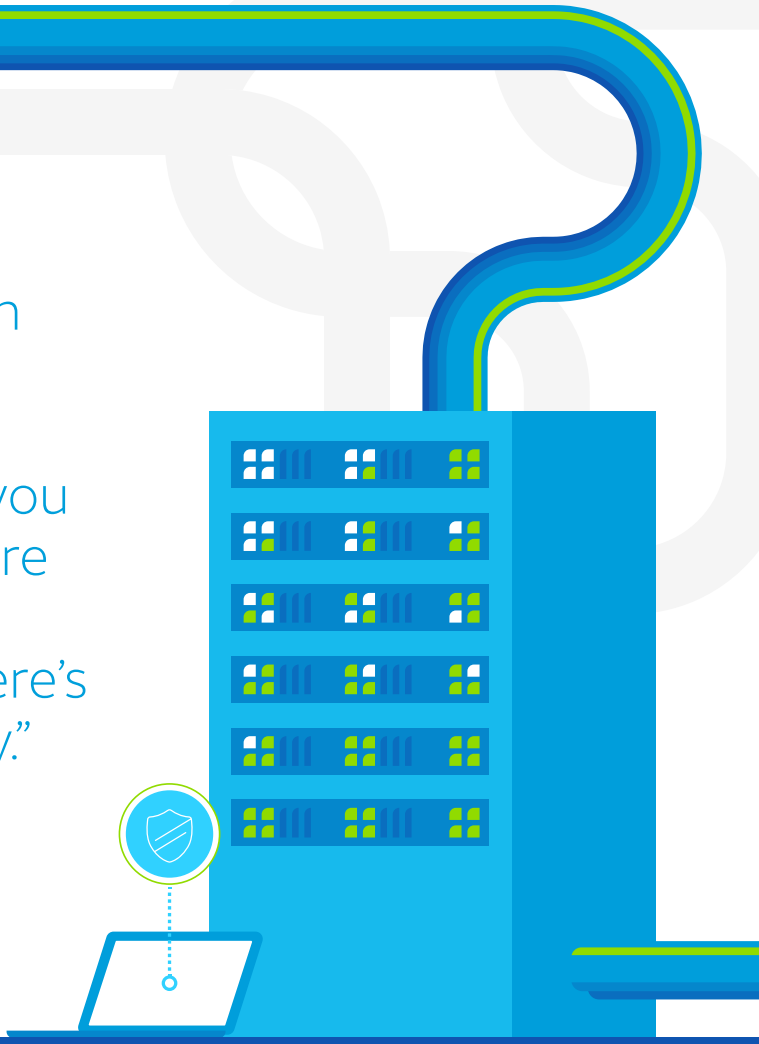
Executive summary

This edition of Cybersecurity Insights focuses on the latest results from an online Cybersecurity Risk & Readiness Assessment developed for AT&T by Spiceworks. The assessment enables IT pros to assess their own practices, strategies, and concerns about security by answering 8 simple questions. The responses to date have been surprising—and unsettling. Answers from the assessment reveal that while individual company deficiencies vary, overall security risks are broad, deep, and span across all business sizes and industries.

The risk assessment, on which this report is based, came from our previous report, **Charting a new course: when investing more in cybersecurity isn't the answer**. We will take a look into the answers from the risk assessment, in which many IT pros feel their organizations are still not prepared for cyberattacks and security breaches. And we will explore what organizations can do to better protect themselves and their customers from attacks happening today, from phishing schemes to ransomware, crypto mining and more, as well as how they can be better prepared for the threats of tomorrow.

"There's only so much you can do. You can fix things as they break. You can fix things as infections are detected, and you can quarantine them; but there are always going to be more coming. It's a 24/7 job and there's only so many hours in the day."

-IT pro[1]



The security and risk landscape:

The rise of modular attacks and the growing impact of cryptocurrency

Increase in attacks in 2018

Looking back, 2018 was a tough year for cybersecurity. There was a 350% increase in ransomware attacks, a 250% increase in spoofing or business email compromise (BEC) attacks, and a 70% increase in spear-phishing attacks on companies.[2] Perhaps the most disturbing news about attacks involved crypto mining, where malware attacks increased by 4,000% in 2018. Crypto mining breaches occur when malicious hacker accesses a user's computer without their permission to mine for digital tokens.[3]

Further, the average cost of a cyber-data breach has risen from $4.9 million in 2017 to $7.5 million in 2018, according to the U.S. Securities and Exchange Commission.[2]

The security landscape is growing increasingly treacherous as hackers of every type continue to evolve their attack strategies to evade detection while maximizing profit from their time and effort. It doesn't matter if it's an organized criminal gang looking to make money from ransomware schemes, covert state-sponsored groups attempting to steal data and disrupt operations, or just malevolent individuals trying to impress others in the hacker community—every bad actor is smarter than they were last year, and better equipped to wreak havoc.

It's not just that they're smarter. Cybercrime has become commercialized, and this means that many of the components of an attack are sold on the dark web. Criminals can now launch cyberattacks without having coding knowledge. In addition, attacks can be launched more quickly, and relaunched very easily with just a slight change. This means criminals can be more "persistent" than ever in trying to breach a network.

This alarming escalation in attacks has led senior management to take notice, with 73% of organizations looking to third-party vendors to help them meet their cybersecurity needs, up 30% from 2016.[4]

IT staff will need to be increasingly proactive in their approach to cybersecurity to keep up with constantly evolving threats. Because even sophisticated defense strategies will not remain effective if they're not regularly tested and kept current.

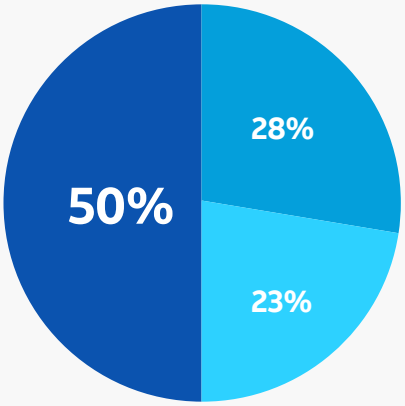
For example, modular malware is becoming a growing concern because it can be released with many variations. To this point, Emotet, an advanced, modular banking Trojan which acts as a downloader to install other malware on a victim's hosts while also stealing sensitive information, has been highly successful. Operators of Emotet initially attack with a malicious email attachment. Once the attachment is successfully executed (by someone opening the attachment), an embedded macro begins requesting the Emotet binary from a malicious destination which then performs a multitude of post-compromise actions. For example, the malware could collect a victim's host details and begin communicating with an attacker-owned command and control (C&C) infrastructure. Once C&C communication is successful, the malware begins downloading and running additional malware as well as updating Emotet over time, thereby expanding its malicious capability.

It's more than just the deviousness of attacks that are evolving, so are the reasons behind them. The WannaCry attack of 2017 demonstrated that cryptocurrency will be a major catalyst in new cyberattacks. Not only are criminals demanding ransom in cryptocurrencies like Bitcoin, but they're now also taking over machines and their computing power for crypto mining.

One of the most widely observed objectives of attacking an organization's cloud infrastructure has been for cryptocurrency mining. Despite recent falls in cryptocurrency prices, mining campaigns continue to plague organizations.[4]

Mining for cryptocurrency requires an enormous amount of raw processing power. Since high-speed processors are expensive, and running them at full power for long periods of time costs even more, criminal elements have started hijacking processing power by deploying clandestine cryptocoin mining code to whole networks of computers. The mining code malware automatically copies itself and continues attempting to infect as many machines as possible.

While the threat landscape gets more treacherous by the day, IT teams seem to be underprepared for the imminent attacks on the horizon, according to the responses from the risk assessment.



Which of the following best describes your organization's cybersecurity program?

- Our security policies are ad-hoc, not risk driven, and not integrated with our overall security goals.
- Our security program is relatively well-defined, including business stakeholders and risk metrics, but we rarely update it.
- Our security program is continuously improved and maintained, includes defined roles and responsibilities, and aligns with risk-driven metrics.

> "I feel somewhat apprehensive in the sense that I feel like we're doing a fairly good job, but it's the fear of the unknown—'What am I missing?'—that's going to cost us in the end."
>
> – IT pro[1]

When asked to describe their organization's cybersecurity program, a stunning 50% of IT pros stated that their security policies were "ad-hoc, not risk-driven, and not integrated with our overall security goals."[4]

This level of disconnection between the security threats that exist today, as well as those to come, in addition to not having the proper tools to understand the threat landscape, should be a major concern to organizations everywhere. While criminal attacks get smarter, many companies seem to be whistling past the proverbial graveyard when it comes to cyber security. And that lack of attention can lead to devastating consequences.

Detection and response:

Identifying suspicious activity and thwarting attacks

Resilient detection and response are critical to organizations that need to quickly and aggressively address any active or potential threat. Indications of wrongdoing can often be identified because of an aberration of normal security protocol. From unusually high traffic across normally unremarkable ports to unidentified users attempting to access secure files, any suspicious activity should immediately be investigated and acted upon.

Without appropriate detection and response strategies, processes, and technologies in place, even seemingly innocuous activity can result in tremendous, costly, and possibly irreparable harm to the organization.

One recent study showed that companies that have been attacked experience a sales decline of sales growth of more than 3 percent.

They are also subject to reduced investment, increased debt (with leverage ratios rising by more than 2 percentage points on average after an attack) and see a reduction in their credit rating.[6]

While it's been commonplace to assume that most companies use tools such as Security Information and Event Management (SIEM) to detect and respond to threats, that is not what we see in the responses to the online risk assessment.

> "You see all these alerts that are coming in and all this traffic. How do you pinpoint what is real? How do you know what you need to focus on versus what is routine traffic?"
>
> – IT pro[1]

How does your organization currently identify cybersecurity threats?

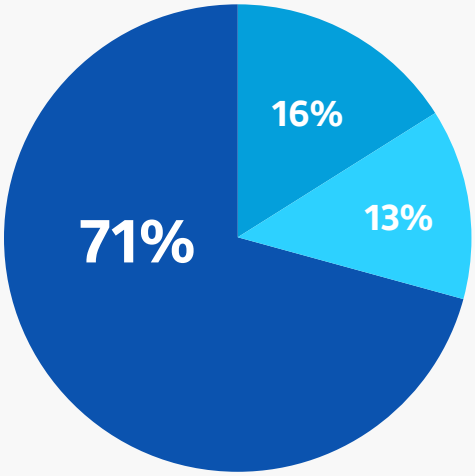
In answering how their organization currently identifies cybersecurity threats, an alarming 63% said that they don't utilize any SIEM tools at all.[4]

Even more distressing was the response to the question, "How does your organization coordinate incident response tasks with internal stakeholders (IT, legal, senior management) and external stakeholders (suppliers, distributors, customers, regulators)?" A soaring 71% of IT pros said their incident response tasks are ad-hoc, manual, and untested, and that they do not have an incident response retainer.[4]

Only 16% of participants report having an incident response retainer, and that the associated tasks were automated and documented.[4]

This lack of detection and response preparedness can be quite risky. Organizations are putting themselves, their partners, and their customers in an excessively vulnerable position by not taking a more thorough and proactive approach to detection and response. And it's hard to believe those same partners and customers would be comfortable knowing how truly susceptible they were to malicious attacks from so many different sources.

IT leadership and senior management must implement solutions to mitigate security threats by proactively identifying suspicious activity and comprehensively auditing their entire approach to security—from both a human and technological perspective. Failure to make these adjustments quickly and system-wide creates an environment ripe for relentless attacks from a broad range of malicious parties.



How does your organization coordinate incident response tasks with internal stakeholders and external ones?

- Our incident response tasks are ad-hoc, manual and untested.
- Our incident response tasks are automated and documented, with a response retainer.
- Our incident response tasks are automated, documented and tested with no response retainer.

Threat intelligence and security management

Knowing about potential threats can help prevent actual attacks

It is no longer acceptable to have a passive approach to threat intelligence. In Cybersecurity Insights Vol. 8, we learned why so many organizations are turning to managed security service providers (MSSPs). For most companies, there is simply too much data to be analyzed. The volume, potency and imperceptible nature of today's attacks make it more difficult than ever to identify a threat.

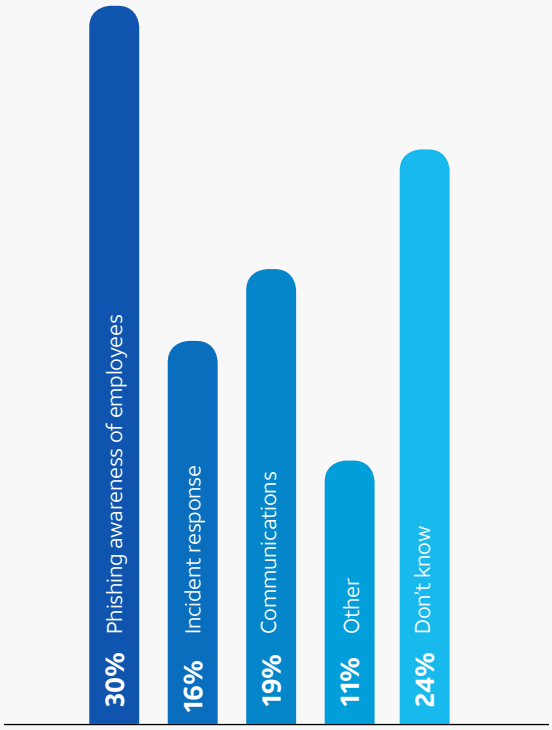
Unless your security team is working toward seeing threats before an attack, you are stuck on the defensive, and forced to respond to the attack as opposed to stopping it before it gets to your enterprise. In essence, threat intelligence is about thinking like the bad guys in order to beat the bad guys.

Threat intelligence can also help IT staff to better understand what security measures need to be in place so that attacks that were successful in the past will be more likely to fail in the future. Good threat intelligence enables security and IT staff to develop resilient threat detection and response, even as the threat actors change their tactics, techniques, and procedures (TTPs) and as their IT system evolves, from moving workloads to the cloud to going "mobile".

There are a number of components involved in building an effective threat intelligence system, including the following:

- Developing a deliberate plan and clear collection strategy are key to ensuring timely and relevant threat intelligence
- Deciding which types of critical intelligence are appropriate for the needs of the organization.
- Considering how that intelligence is gathered
- Determining whether or not to work with a threat intelligence vendor to assist in threat data collection
- Providing security teams with a means to process and analyze their threat data so they can consume and disseminate throughout their security tools
- Developing a process for continuous updating and feedback to stay on top of emerging and evolving threats as the threat landscape and your organization's infrastructure changes

Feedback on threat intelligence from the online risk assessment suggested that many companies lack an understanding of the importance of threat intelligence and the catastrophic breaches that can result.



Which elements of human security does your organization test?

The human factor

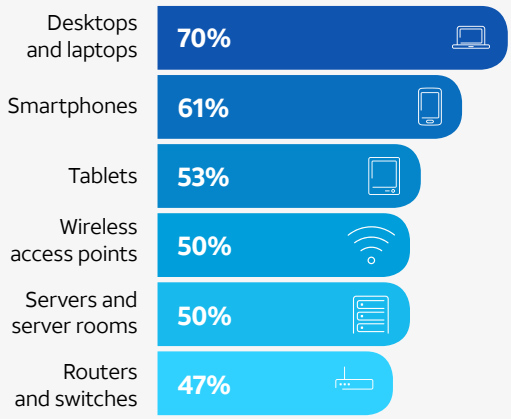
While cybercriminals become more refined in their attack strategies, many still rely on phishing schemes as the most effective way to penetrate an organization. So, it was surprising when the assessment revealed that, according to respondents, only 30% of companies test employees' awareness of phishing schemes. An additional 24% of participants didn't know if their organization conducted any tests to detect if workers are aware of security threats.[4]

When only 1 out of every 3 companies is communicating to employees about the dangers of suspicious emails, and IT pros at 1 out of every 4 companies don't know if there is any effort at education or interdiction, it reveals a massive level of vulnerability to these organizations.

Endpoint sensors

Endpoint devices have become a favorite target of hackers in the past few years, as the number of these devices has exploded. Endpoint devices are most commonly used by end users, and include everything from desktops and laptops to tablets, smartphones, and printers, as well as the growing number of IoT devices. In fact, the only common denominator among endpoint devices is that they are all connected to a network, and therefore of great interest to hackers.[7]

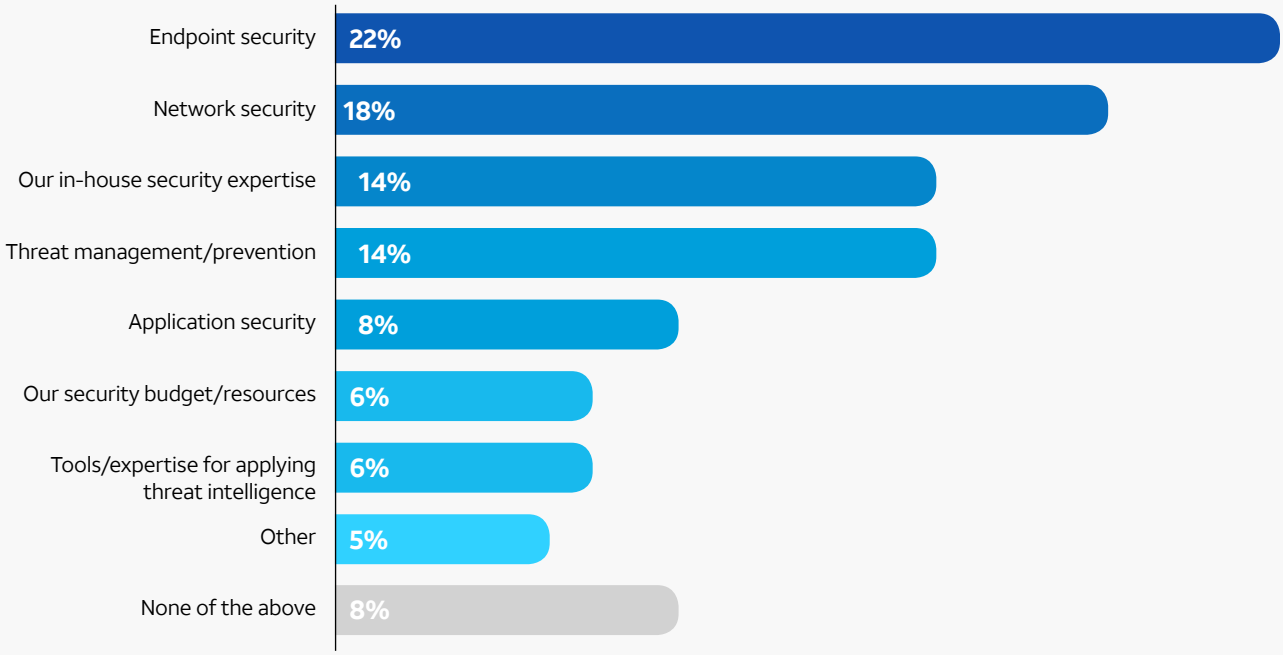
Level of risk for security threat/breach



"Endpoint devices—PCs, printers, scanners, Voice over Internet Protocol phones and smart meters, among others—are increasingly preyed upon by cybercriminals to gain access to sensitive and private information."

– BizTech Magazine[7]

Which areas do you feel most confident about when it comes to remediating or mitigating cybersecurity incidents?



Our research showed that many IT pros are uncertain about the level and effectiveness of their organizations' approaches to endpoint security threats.

For companies to succeed in defending endpoint devices, they need to deploy security tools, such as application-based threat protection, to block malware. They need network-based threat protection which can be used against Man-in-the-Middle and SSL attacks. And they need to utilize device-based threat protection to block "jailbreaks," OS vulnerabilities, and inadequate device configurations.

When asked, "Which areas do you feel most confident about when it comes to remediating or mitigating cybersecurity incidents?" **only 22% of respondents expressed confidence about endpoint security.**[4]

Cybersecurity in the cloud

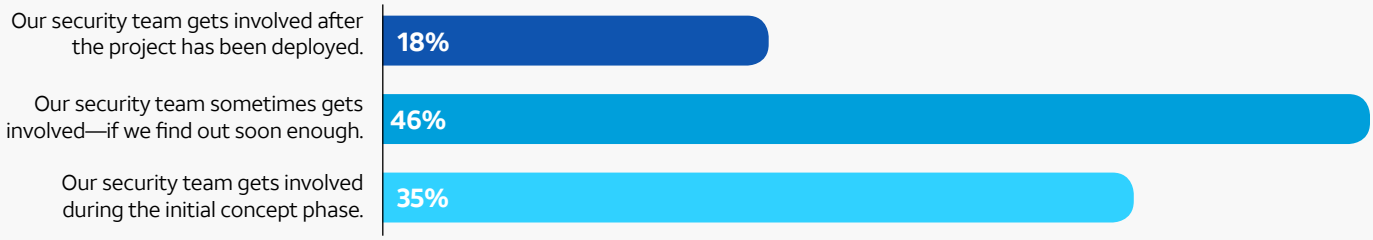
While the cloud continues to expand at a seemingly exponential rate, IT pros who took the online risk assessment are still struggling to understand the risks, strategies, and potential benefits of utilizing the cloud to protect their organizations' data and networks.

In responding to the question, "How do you understand the cybersecurity risks as you deploy emerging technology (cloud, mobility, IoT)?" less than half (46%) stated that the security team "sometimes get involved, if they find out soon enough."

Almost 20% responded that they get involved only after the project has been deployed.[4]

At least some companies seem to comprehend the importance of the cloud when it comes to cybersecurity, as 35% of respondents said that their security team was involved in the initial concept phase of cloud migration.[4]

How do you understand the cybersecurity risks as you deploy emerging technology (cloud, mobility, IoT)?



Penetration testing

In seeking new and smarter ways to improve cybersecurity, penetration testing (pen testing) is gaining a reputation as a vital tool for organizations attempting to stay ahead of hackers. Pen tests are used to measure the effectiveness of security in areas such as network configuration, encryption, and authentication, and the vulnerability of end user devices.

> "One of the most important activities that organizations can do to prepare for potential cyberattacks is to conduct penetration testing exercises. Regular penetration testing is so important for preparedness that it's a requirement in the Payment Card Industry Data Security Standard (PCI-DSS)."[8]

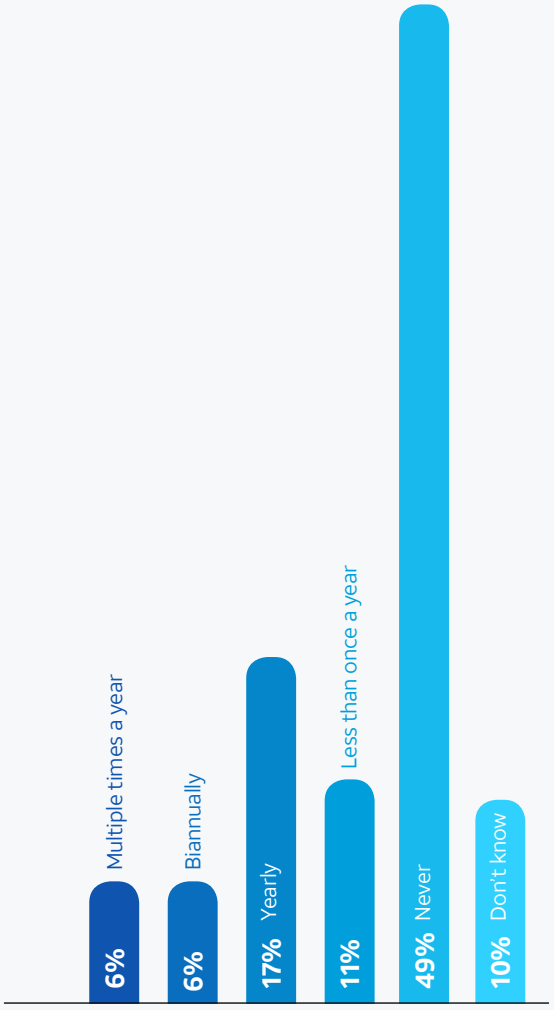
How important is pen testing?

According to a recent survey of professional hackers who conduct pen tests, 88% said that they could infiltrate an organization and exfiltrate target data within 12 hours.[9]

Those who took the online risk assessment indicated that pen testing still had a long way to go in many companies just to gain awareness. In answering the question, "How frequently does your organization conduct IT penetration tests?" an astounding 49% of respondents said "never."

Less than a third (29%) said that they tested 1 or more times a year—the timeframe generally recommended by security experts.[4]

These risk assessment responses reflect just how far many organizations still need to go in putting together the strategies, technologies, and rigorous verification processes required to meet the malevolent security attacks that exist today, and those that will intensify in both severity and volume in the years ahead.



How frequently does your organization conduct IT penetration tests?

It's time to get serious about cybersecurity

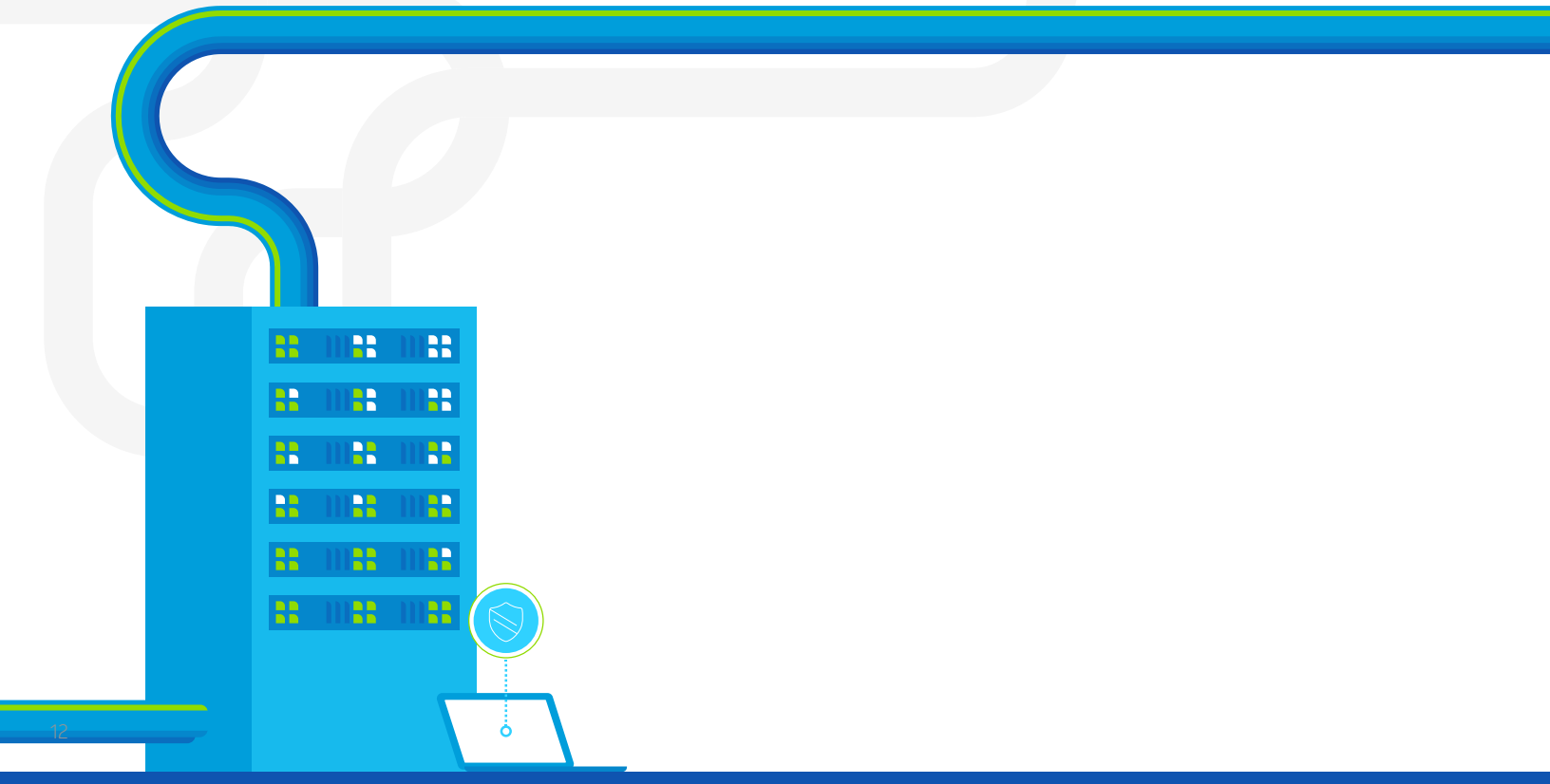
The days of hoping to simply avoid cyberattacks are long gone. The threats are real and the damage they can inflict is incalculable. And nobody will tolerate excuses. Not senior management. Not shareholders. Not customers.

It also must be noted that security is not a fix-it-and-forget-it proposition. It's a 24/7 issue that will need to be (revisited) regularly to provide that the defenses are as state-of-the-art as the attacks.

That's why AT&T has created edge-to-edge technology solutions that provide near-real-time intelligence from every corner of an organization's enterprise, hardware to software, devices to people. We offer cybersecurity solutions that utilize our unrivaled visibility into networks to help enable companies to anticipate, identify, and proactively defend against threats before damage is done or data is stolen.

"Cybercriminals are always evolving and changing their TTPs (tactics, techniques, and procedures) to avoid detection and take advantage of a bigger return on their investment, or simply take the path of least resistance. That's why organizations need to stay on top of the threat intelligence that's feeding their security controls, continuously updating it with new information as well as internal and external feedback. This will ensure resiliency in threat detection even as cybercriminals change their approach."

- Jaime Blasco,
  Vice President and Chief Scientist,
  AT&T Cybersecurity



AT&T Alien Labs includes a global team of threat researchers and data scientists who, combined with proprietary technology in analytics, automation, and machine learning (ML), analyze one of the largest, most diverse collections of threat data in the world to provide curated threat intelligence ¬that is the foundation of AT&T Cybersecurity. We know that almost all cybersecurity breaches occur in the "seams" between people, processes, and technologies.

It's why we take a "full stack" approach to cybersecurity, including consulting, managed services, threat detection, and response, along with integration, orchestration, and automation.

Conclusion

AT&T Cybersecurity technologies provide phenomenal threat intelligence, collaborative defense, and security without the seams to help you protect your business regardless of size or industry. Our unique approach integrates best-of-breed technologies that offer unrivaled network visibility plus actionable threat intelligence from Alien Labs researchers, Security Operations Center analysts, and machine learning. It's what we consider an edge-to-edge approach to cybersecurity, providing solutions to fit—and protect—your business.

Keep up-to-date

Stay on top of the latest cybersecurity advancement, issues and discussion among thought leaders by reviewing all of our security reports at **att.com/cybersecurity-insights**.

Ready for your own cybersecurity risk assessment?

Find out where your organization stacks up in regard to cybersecurity by taking the **Cybersecurity Risk & Readiness Assessment**. You can see how well prepared you are to address threats and determine where you need to make improvements.

Learn how AT&T security solutions can help you at: **att.com/security**

AT&T Business

Sources:

[1] AT&T Cybersecurity Vol. 8 Content Research Interviews, Spiceworks Research Report, August 2018.

[2] Gregory Garrett, "Cyberattacks Skyrocketed in 2018. Are you ready for 2019?" *IndustryWeek*, December 13, 2018. https://www.industryweek.com/technology-and-iiot/cyberattacks-skyrocketed-2018-are-you-ready-2019

[3] Donna Fuscaldo, "Crypto Mining Malware Grew 4,000% This Year," *Forbes*, December 2018 https://www.forbes.com/sites/donnafuscaldo/2018/12/28/crypto-mining-malware-grew-4000-this-year/#601acd48224c

[4] AT&T Cybersecurity Risk & Readiness Assessment. https://community.spiceworks.com/partners/att/cybersecurity-risk-assessment

[5] Chris Doman and Tom Hegal, "Making it Rain – Cryptocurrency Mining Attacks in the Cloud," AT&T Security Blogpost, March 2019 https://www.alienvault.com/blogs/labs-research/making-it-rain-cryptocurrency-mining-attacks-in-the-cloud

[6] Peter Orszag, "Effects of Cyber Breaches on Corporate Bottom Line," Insurance Journal, April 2018. https://www.insurancejournal.com/news/national/2018/04/13/486383.htm

[7] Christoph Ruef, "3 Best Practices to Boost Endpoint Security," *BizTech Magazine*, February 2019. https://about.att.com/story/att_threat_intellect.html

[8] Sean Michael Kerner, "One third of companies are largely unprepared for cybersecurity attacks," *eSecurity Planet*, February 2019. https://www.esecurityplanet.com/threats/one-third-of-companies-unprepared-for-cyber-attacks-survey.html

[9] Davey Winder, "Penetration tests are being ignored by enterprises living dangerously," *SC Media UK*, February 2017. https://www.scmagazineuk.com/penetration-tests-ignored-enterprises-living-dangerously/article/1475231

© 2019 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.