MIND THE GAP:
CYBERSECURITY'S BIG DISCONNECT

THE CEO'S GUIDE TO CYBERSECURITY

AT&T Business

Cybersecurity risks are escalating.
So why do so many organizations continue to miss the mark in defending against them?

Contents

4 *Introduction*

5 *Confronting an Evolving Threat Landscape*

8 *Cyberinsurance Is Not Equal to Cybersecurity*

10 *Shortage? What Skills Shortage?*

14 *The Weakest Link*

16 *Best Practices for Closing the Gaps*

21 *Summary*

22 *Additional Reading*

22 *Sources*

For more information:

Visit us at att.com/cybersecurity-insights
Follow us on Twitter @attbusiness

Cybersecurity technologies and practices are constantly evolving to help organizations defend against persistent and increasingly malicious cyberthreats. But there's more work to be done. Notable disconnects have emerged between ever-shifting cybersecurity threats and organizations' countermeasures.

AT&T's 2017 Global State of Cybersecurity survey uncovers some critical gaps in current cybersecurity strategy that, if left unchecked, could provide an open door to cybercriminals:

- Twenty-eight percent of organizations appear to view cyberinsurance as a substitute for cyberdefense investment, rather than as one component of a multilayered cybersecurity strategy.
- Two-thirds of organizations say their in-house cybersecurity capabilities are adequate to protect against cyberthreats, yet nearly 80% say they have been breached within the past year.
- Just 61% of organizations mandate cybersecurity awareness training for all employees, while more than half admit to breaches from employee mobile devices infected with malware.

This report examines the implications these potential vulnerabilities present and the steps CEOs and their cybersecurity teams can take to help strengthen their approach and reduce risk across the business.

Ponemon Institute estimates the average cost of a data breach in 2017 was

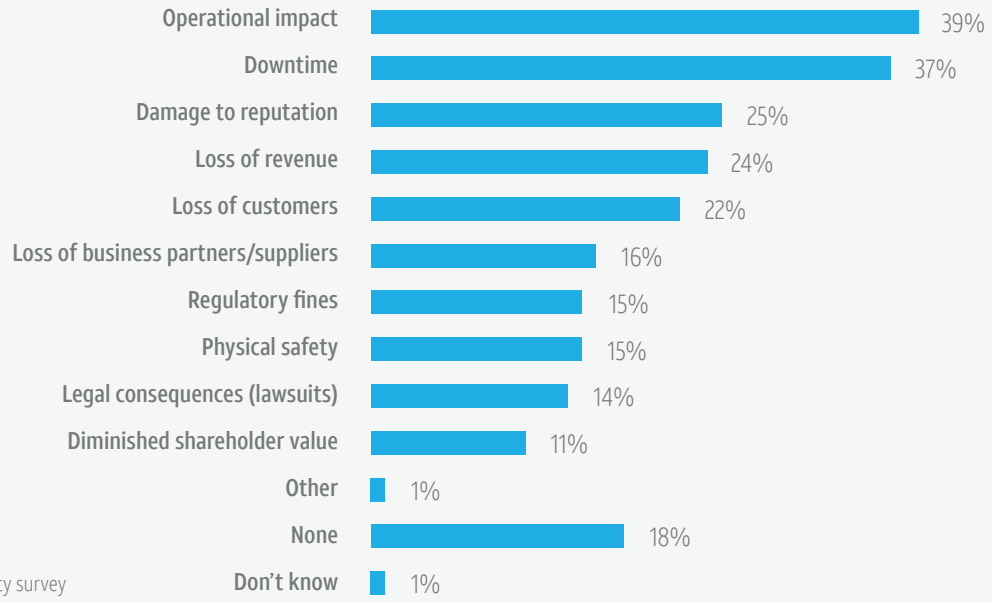
$3.6 million.

Confronting an Evolving Threat Landscape

All organizations are vulnerable to cyberattack — no matter their size, type or location. Appropriately, many have proactively invested in cybersecurity defense. And yet troubling gaps have emerged between the rapidly evolving threat landscape and the resources organizations are allocating to defend against cyberattacks.

According to the 2017 AT&T Global State of Cybersecurity survey, a cybersecurity attack has negatively affected nearly 80% of surveyed organizations in the past 12 months. The impact touches virtually every aspect of business.

How has a cybersecurity attack or successful breach affected your organization?



Source: AT&T 2017 Global State of Cybersecurity survey

The damage can add up quickly: Ponemon Institute estimates the average cost of a data breach in 2017 was $3.6 million[1]. Other studies show that a quarter or more of shareholder value may rely on a company's reputation[2]. Clearly, organizations can't afford to ignore either the tangible or intangible damage resulting from a cyberbreach.

Today's leadership now understands the variety of business risks from cyberattacks. What's notable is the disconnect in how organizations are addressing these threats. Three areas of concern emerge from the AT&T survey:

Overreliance on cyberinsurance

Overconfidence in internal capabilities

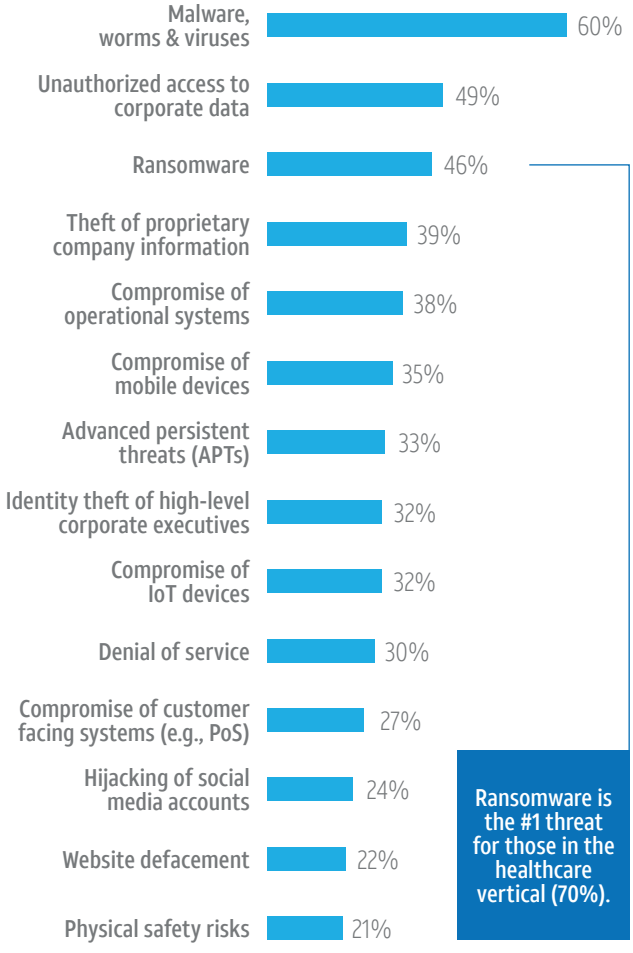
Underappreciation of cybersecurity awareness training

Deep Dive: Persistent, Emerging Threats

The variety and volume of cyberattacks continue to increase, exacerbating cybersecurity challenges from one year to the next. Malware and unauthorized access to corporate data remain chief concerns, but these persistent threats are joined by growing risks associated with the Internet of Things (IoT), ransomware, mass destruction malware and mobile devices.

More than one-third (35%) of all the respondents to the AT&T survey — a number that increases to nearly half (46%) for organizations in Asia-Pacific (APAC) — say IoT devices were the primary source of a data breach experienced over the prior year.

Organizations' top perceived threats in the year ahead



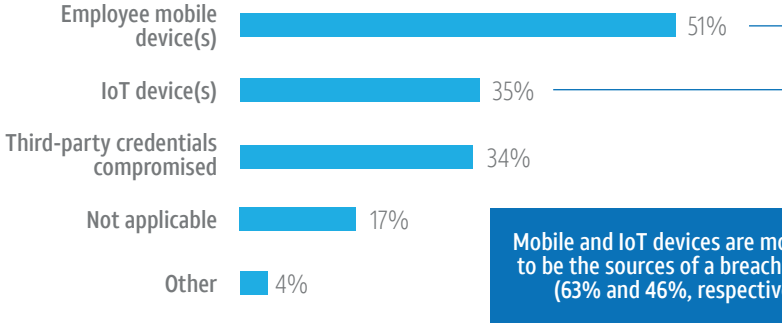
Source: AT&T 2017 Global State of Cybersecurity survey

The outlook for future IoT attacks remains bleak, with 68% of survey respondents (and 78% of APAC organizations) expecting IoT threats to increase in the coming year.

An equally pressing danger — ransomware — has eclipsed almost all other cyberthreats as a top concern. Nearly half (46%) of survey respondents cite concern for ransomware, in which files are encrypted and the attacker demands a digital ransom to unlock them — with no guarantee that a payment will actually result in the affected files being unlocked. Notably, this form of attack is now the top concern within the healthcare sector, with 70% of respondents listing it as a major threat.

Cybercriminals have extended the reach of ransomware, malware and other malicious software by taking advantage of the growth of smartphones and tablets. Employee mobile devices were the primary source (51%) of breaches due to the exploitation of known vulnerabilities over the past year. In the coming year, nearly three-quarters of survey respondents expect threat levels to increase for data stored in mobile devices and apps.

Primary source of data breaches in the past 12 months



Mobile and IoT devices are more likely to be the sources of a breach in APAC (63% and 46%, respectively).

Source: AT&T 2017 Global State of Cybersecurity survey

Cyberinsurance Is Not Equal to Cybersecurity

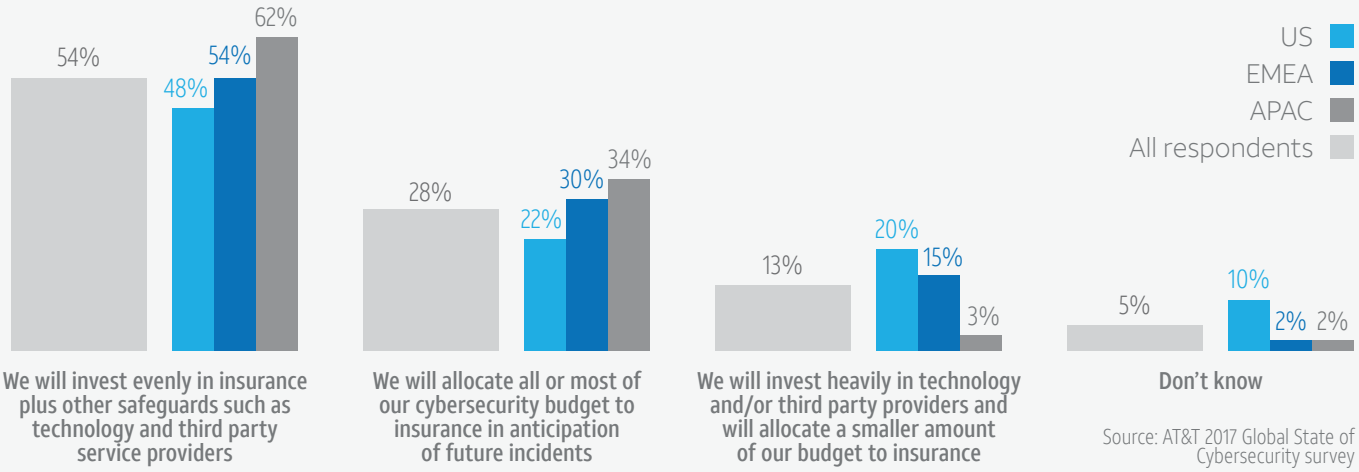
84%
of organizations have purchased cyberinsurance or plan to do so.

Acknowledging the seeming inevitability of a successful cyberattack on their organization, many business leaders are turning to cyberinsurance as a hedge against losses resulting from a breach. In fact, 84% of organizations in the AT&T survey have already purchased cyberinsurance or plan to do so.

While utilizing insurance to transfer financial risk is foundational to a complete risk management strategy, it does not eliminate risk and should be used in combination with a robust cybersecurity plan to manage retained risk. Not surprisingly, insurance plans that cover some financial losses caused by cyberattacks are increasingly being adopted as part of risk management strategies that also include cybersecurity.

Nearly 3 in 10 survey respondents (28%) plan to allocate all or most of their cybersecurity budget to insurance in anticipation of future incidents. Among APAC organizations, the number rises to 34%. For companies in the technology sector, 43% plan to allocate all or most of their cybersecurity budget to insurance.

How organizations plan to utilize cybersecurity insurance



Source: AT&T 2017 Global State of Cybersecurity survey

Key Takeaway: Cyberinsurance

An overreliance on cyberinsurance alone raises concerns on several levels. First, it can divert attention (and investment) away from critical resources required to address threat protection, detection and response. In addition, while cyberinsurance can help recoup financial losses that stem from a successful breach, it may not mitigate other impacts including business downtime, reputational damage or customer attrition.

Leadership also needs to have a clear understanding of the rules and regulations governing insurance coverage, as well as the fine print of policy coverages and exclusions. Many organizations that successfully acquire cyberinsurance as part of their risk management strategies often have existing cyberdefense programs.

While cyberinsurance has a growing role in mitigating many of the financial risks inherent in a successful breach, it can't prevent a cyberattack. As with any insurance, you must demonstrate that the cybersecurity controls in place at the time of purchase remained in place at the time of breach for reimbursements to follow. To get the most out of any investment, insurance should be part of a more comprehensive risk management program that includes comprehensive cyber risk assessment, mitigation and ongoing monitoring. That way, leadership will have the information it needs to make coverage decisions that deliver the best possible outcome in case of attack.

Shortage? What Skills Shortage?

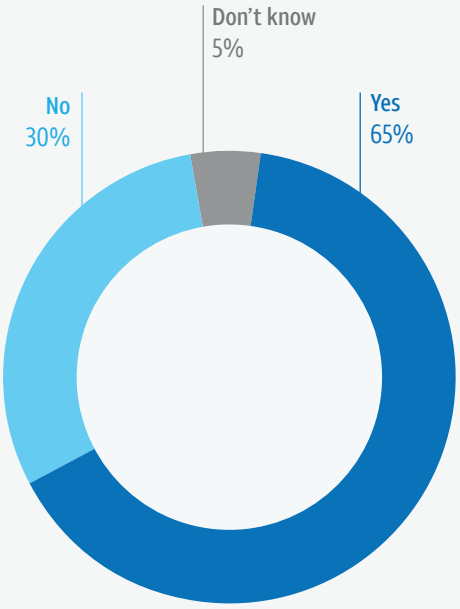
Despite the array of cyberthreats, many organizations remain stubbornly optimistic about their abilities to counter the risks. Nearly two-thirds (65%) of respondents to the AT&T survey say they have adequate in-house talent to address their cybersecurity needs in the year ahead — even though 80% admit to experiencing a negative impact from an attack in the previous 12 months. Senior executives are particularly confident, with 70% of C-level respondents saying they have adequate talent, vs. 56% of those closer to the front lines. That's a troubling gap between leadership and the front-line charges who are tasked with defending against known and unknown threats.

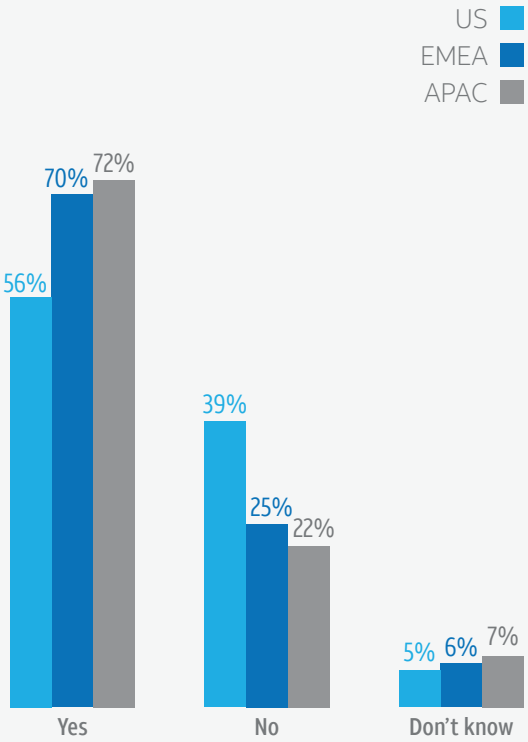
65% of IT and cybersecurity leaders say they have adequate in-house talent to address their cybersecurity needs in the year ahead — even though 80% admit to experiencing a negative impact from an attack in the previous 12 months.

U.S. respondents are arguably more pragmatic than their overseas counterparts. Just 56% of the U.S. respondents professed confidence in their ability to address cybersecurity challenges internally, compared to 70% of respondents in EMEA and 72% in APAC.

In spite of these brave fronts, at least half of all organizations surveyed admit they face skills gaps in three key areas: threat prevention (56%), threat detection (50%) and threat analysis (50%). Threat prevention is a particularly scarce resource in APAC and EMEA, with 64% of respondents from each of these regions citing a lack of in-house skills.

Is your organization's in-house talent adequate to address your cybersecurity needs over the next 12 months?





Source: AT&T 2017 Global State of Cybersecurity survey

Deep Dive: Staffing Plans by Region

Even though the majority of organizations in the AT&T survey express confidence in their existing in-house capabilities, half plan to increase their cybersecurity staff over the next 12 months. These plans vary by region, with 66% of APAC-based respondents planning staff additions, compared to 46% of U.S. firms and 41% of EMEA companies.

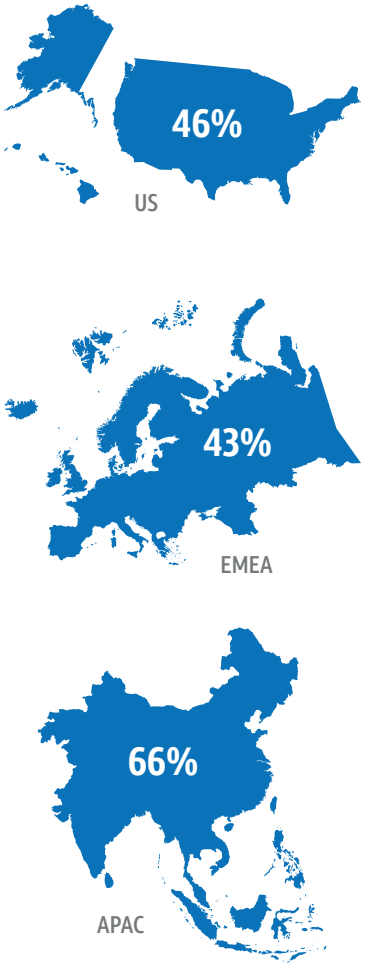
On average, those expecting to bolster their cybersecurity staff anticipate an average increase of 24% in the U.S., 21% in APAC and 15% in EMEA.

For all three regions, companies in the technology and healthcare sectors plan the biggest increases, with companies in both expecting to expand their cybersecurity personnel numbers by 27%.

Regional differences also exist when it comes to supplementing in-house talent with managed services providers and third-party consultants. U.S. respondents are the least likely to rely on managed service providers and consultants, with nearly two-thirds of their needs addressed by in-house staff.

APAC-based organizations are the most open to outside assistance, expecting 27% of their needs to be met by managed services providers, 22% by consultants and just 46% by in-house talent. EMEA-based companies fell in the middle: 24% managed services providers, 18% consultants and 54% in-house.

Plans to increase in-house cybersecurity staff in the next 12 months



Source: AT&T 2017 Global State of Cybersecurity survey

Key Takeaway: Staffing

When it comes to staffing, the numbers don't add up. CEOs need to have frank discussions with their cybersecurity leadership teams about current in-house capabilities, gaps and investments. Regardless of company size, cybersecurity has become a dynamic, moving target, requiring trusted service providers and other entities.

Consultants and managed service providers have the advantage of specializing in cybersecurity. These providers are often able to attract top-notch talent and implement cutting-edge cybersecurity technologies faster. Given that the U.S. has a reported skills gap of 300,000 cybersecurity experts, these providers can serve as resources of much-needed talent[3].

In addition, service providers have a unique view across multiple customers with a broad range of business and cybersecurity requirements. With massive volumes of network activity housed in their data lakes, cybersecurity service providers can deploy analytics that generate deep insights about the threat landscape — knowledge that can benefit all of their customers. When a provider identifies an attack directed at one of its customers, it can help all of its customers recognize and defend against the same form of attack.

CEOs

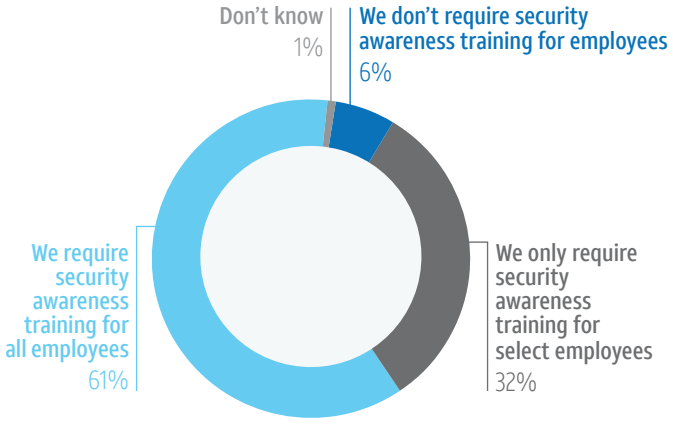
need to have frank discussions with their cybersecurity leadership teams about current in-house capabilities, gaps and investments. Regardless of company size, cybersecurity has become a dynamic, moving target, requiring trusted service providers and other entities.

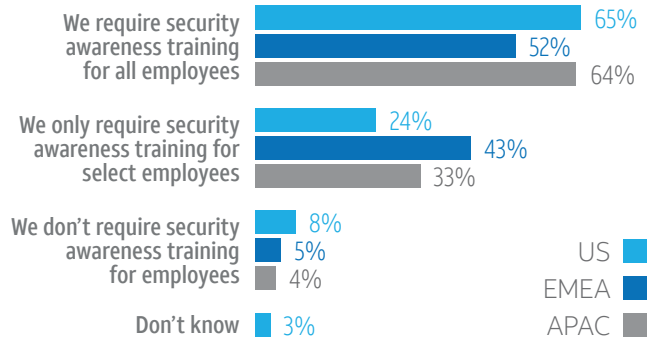
The Weakest Link

Companies with strong defenses and experienced in-house or third-party cybersecurity teams still routinely fall victim to network, system or data breaches. This reality points to another disconnect: employees' role in breaches vs. the type and cadence of cybersecurity awareness training designed to educate the workforce on the risks.

As noted earlier, employee mobile devices were the primary source of more than half of the known data breaches during the past year (63% of breaches in APAC). Nearly three-quarters of survey respondents expect increasing threats to data residing on mobile apps, mobile devices and cloud-based applications. These alarming statistics point to the importance of conducting ongoing employee cybersecurity awareness and procedures training to

Security awareness training for employees





Source: AT&T 2017 Global State of Cybersecurity survey

help prevent breaches to the enterprise through exposure by employee mobile devices and apps.

Yet, despite widespread acknowledgement that employee awareness is critical, there's still a big gap in execution. Just 61% of organizations in the AT&T survey require cybersecurity awareness training for all employees. That percentage drops to just 52% of EMEA-based organizations, with 43% saying they require cybersecurity training only for select employees (compared to 24% of U.S. firms and 33% of APAC organizations).

Cybersecurity training practices also vary by sector and in surprising ways. For example, while 61% of all organizations in the AT&T survey require across-the-board cybersecurity training, only 56% in banking and finance — a frequent target — require such training.

Key Takeaway: Awareness Training

Employee awareness is not a simple check-the-box exercise. Companies must invest in comprehensive, ongoing programs to minimize the weakest link syndrome. In this regard, workforce-wide cybersecurity training is only the first step. Reinforcing and testing of the awareness training over time will also allow for optimization and point to where knowledge gaps exist. Post-test evaluations and ongoing improvements are also required to fully realize the benefits of cybersecurity awareness training.

Best Practices for Closing the Gaps

Crafting a cybersecurity strategy is a complex exercise that involves aligning cybersecurity requirements to business objectives, and then matching investments against the risk profile derived from an understanding of the threat landscape. Organizations have made significant headway in creating multiple layers of defense, detection and mitigation. But there's still plenty of work to do to tighten up vulnerabilities and reduce the risk of a devastating attack. If you're concerned about any of the disconnects we've identified in this report, here are four best practices to help you get your strategy back on track.

1 Expand risk assessment programs to account for increasingly digital business models

A cyber risk assessment helps you to determine how to best apply your current and future cybersecurity investments. It's a positive sign that 90% of the organizations AT&T surveyed said they have conducted enterprisewide cyber risk assessments in the past year.

Less encouraging: Only 50% have conducted risk assessments specific to IoT threats, despite acknowledgment that these threats are significant and escalating.

90% of organizations have conducted enterprisewide cyber risk assessments in the past year, but just 50% have conducted risk assessments specific to IoT threats.

Even general cyber risk assessments can be undercut by poor assessment practices. Ideally, organizations should create a feedback loop between cybersecurity operations and a flexible risk management strategy that evolves based on daily threat activity and response. At present, just one-third of all organizations in the AT&T survey conduct ongoing cyber risk assessments.

It's important also to include an evaluation of the cybersecurity posture of third-party consultants, vendors and other entities in your cyber risk assessments. Among those surveyed, slightly over half (54%) have a formalized risk management program in place for third parties (68% of those in the technology sector), and another 37% plan to implement one.

54%
of organizations have a formalized risk management program in place for third parties, and 37% plan to implement one.

2 Don’t go it alone when it comes to building and maintaining cybersecurity defenses

In-house cybersecurity teams are very important, but they are rarely sufficient on their own to defend against constantly evolving and escalating cyberthreats. Cybersecurity has become a team sport that requires trusted service providers and other entities. Build relationships with vendors who can become true strategic allies — especially those that can apply visibility, expertise and insights gained from a large customer base to your specific cybersecurity risks and challenges.

Not going it alone also means not turning your back on the trend of increasing cybersecurity intelligence and automation. In an era of critical cybersecurity staff shortages and daily cybersecurity events numbering in the millions, automation is a necessity, not a luxury. Increasingly, automation will reach beyond its current sweet spot of threat identification and alerting into the realm of automated threat response and mitigation.

3 Formalize awareness training and testing across — and outside — your organization

We can't stress enough that any employee represents a potential attack target. The costs of educating your full workforce about cybersecurity threats and best practices are trivial when weighed against the potential damage and expense a cyberbreach can cause. In this regard, technology companies are leading the way, with 71% of respondents in this vertical providing cybersecurity training to all of their employees.

When it comes to cybersecurity training, though, organizations must look beyond their own walls. In today's interconnected digital world, it's important to evaluate — and bolster — the cybersecurity of third-party consultants, vendors and other entities that handle your data or have access to your networks. In one promising sign, the AT&T survey found that 66% of the respondents include vendors and contractors in their awareness training programs.

All cybersecurity training must be followed by testing, post-test evaluations and ongoing improvements.

4 Invest strategically to strengthen your overall cybersecurity

A sophisticated cybersecurity strategy relies on investing in the right mix of defense tools and mitigation plans. Basic blocking and tackling is only one part of the strategy. All businesses must recognize the inevitability of a breach and invest in countermeasures that will mitigate potential damage, whether financial or reputational. Consider these approaches:

- **Consider cyberinsurance as part of a comprehensive risk management plan.** To limit financial losses in the event of a breach, consider pairing appropriate cyberinsurance coverage with a comprehensive and well-tested cybersecurity plan.

- **Balance prevention, detection and remediation.** The AT&T survey reveals that cybersecurity technology investments are weighted toward prevention (43% of investments), with smaller portions dedicated to monitoring and detection (33%) and remediation after an attack occurs (24%). It's important to find the right balance of these critical investments based on your organization's risk profile and the evolving threat landscape.

- **Stay current on emerging technology.** Even those organizations that lean heavily toward cybersecurity technology can struggle to keep pace with the rapid advances in the cybersecurity defense marketplace. Fortunately, most organizations are making an effort to stay abreast of new cyberdefense tools and approaches. More than two-thirds (70%) of those surveyed by AT&T plan to increase their investments in next-generation cybersecurity technologies, including threat analytics, cloud cybersecurity solutions and machine learning.

Summary

Last year's cybersecurity strategy may no longer be effective for the year ahead. To keep pace with the evolving threat landscape, CEOs and their leadership teams need to fill any large gaps in their approach while constantly fine-tuning their investments and practices.

There's nothing an organization can do to end the cybersecurity threat completely. But a fluid, multilayered approach will help CEOs better focus cybersecurity investments to help protect against the next cyberattack — wherever it may come from.

Respondent Profile

About the Global State of Cybersecurity survey

IDG Research conducted the Global State of Cybersecurity survey on behalf of AT&T in May 2017. To qualify, survey respondents were required to work in an IT/IT Security function at director-level or above and be directly involved in decision making for IT security solutions.

Organization Size

100,000 or more	**6%**
50,000–99,999	**5%**
30,000–49,999	**8%**
20,000–29,999	**10%**
10,000–19,999	**9%**
7,500–9,999	**7%**
5,000–7,499	**8%**
2,500–4,999	**16%**
1,000–2,499	**18%**
500–999	**9%**
250–499	**4%**

Job Title

IT Management	**100%**
CIO	**28%**
CTO	**17%**
CSO, CISO	**11%**
COO	**3%**
Senior Architect/Architect	**5%**
SVP, EVP, VP	**9%**
Director	**28%**

Mean number of employees	**18,729**
Median number of employees	**5,862**

Top Represented Industries

Manufacturing/Industrial	**14%**
Technology	**12%**
Banking & Financial Services	**12%**
Business/Professional Services	**9%**
Healthcare	**7%**
Information, Media & Entertainment	**6%**
Retail Trade	**5%**
Chemicals/Energy/Utilities	**4%**
Transportation & Logistics	**4%**
Government/Public Sector	**4%**
Life Sciences, Pharma, Biotechnology	**4%**

Total Respondents	**700**
US	**300**
EMEA (France, Germany, Italy, UK)	**200**
APAC (Australia, China, Japan, Hong Kong, Singapore)	**200**

Additional Reading

- Cybersecurity Insights, vol. 1: What Every CEO Needs to Know About Cybersecurity www.business.att.com/cybersecurity/archives/v1
- Cybersecurity Insights, vol. 2: The CEO's Guide to Securing the Internet of Things www.business.att.com/cybersecurity/archives/v2
- Cybersecurity Insights, vol. 3: The CEO's Guide to Cyberbreach Response www.business.att.com/cybersecurity/archives/v3
- Cybersecurity Insights, vol. 4: The CEO's Guide to Navigating the Threat Landscape www.business.att.com/cybersecurity/archives/v4
- Cybersecurity Insights, vol. 5: The CEO's Guide to Data Security www.business.att.com/cybersecurity/archives/v5
- Executive Abstracts www.business.att.com/cybersecurity/abstracts
- Cybersecurity Solutions www.att.com/security

Sources

1. IBM/Ponemon, 2017 Cost of a Data Breach. (2017). https://www.ibm.com/security/data-breach/
2. Cole, S., "The Impact of Reputation on Market Value," World Economics, Vol. 13. (July-Sept. 2012). http://www.reputationdividend.com/files/4713/4822/1479/Reputation_Dividend_WEC_133_Cole.pdf
3. CBS News, W.H. Cybersecurity Coordinator Warns Against Using Kaspersky Lab Software. (Aug. 22, 2017). https://www.cbsnews.com/news/kasperksy-lab-software-suspected-ties-russian-intelligence-rob-joyce/

att.com/cybersecurity-insights