2022 Edition

CYBERSECURITY: CONFIDENCE OR CRISIS?

pillsbury

Mergermarket

CONTENTS

FOREWORD & METHODOLOGY

Foreword

Cybersecurity is a constantly moving target. It is estimated that annual losses resulting from cyber threats will total $10.5 trillion globally by 2025—up from $3 trillion in 2015, according to specialist research group Cybersecurity Ventures—forcing continuous investment by businesses and governments in their defenses.

The challenge has only been made greater over the past two years. Technology consultancy Gartner estimates that 60% of knowledge workers are working remotely and nearly a fifth will not return to the office. This, combined with the ubiquitous adoption of cloud services and digitally integrated supply chains, has expanded the available attack surface for bad actors to penetrate. Add to that worsening geopolitical relations and the potential for state-backed corporate espionage, and it is clear that the cyber challenge has never been more pressing.

Companies are not equally prepared to rise to the occasion. For example, businesses in more digitally native sectors such as technology, media & telecoms (TMT) and financial services are better adapted than historically analog industries such as energy, mining & utilities (EMU), our research shows. This report was produced to understand these intricacies and how companies are steeling themselves against rising cyberattacks. We sought to learn about the investments that organizations are making in their technical defenses, their adoption of related insurance coverage, and how they view the threat landscape in the short and medium term.

Methodology

In Q2 2022, Mergermarket surveyed 150 corporate executives divided equally between the financial services, EMU, and TMT sectors, with all organizations having a minimum annual revenue of $500 million. Of the 150 respondents, 120 were based in the United States and 30 in Europe. These included 50 CEOs, CFOs or board members, 50 in-house counsel, and 50 CSOs, CISO, CTO or data protection officers. All responses are anonymous, and results are presented in aggregate.

pillsbury

KEY FINDINGS

While the vast majority of TMT (86%) and financial services executives (80%) are confident in their existing cybersecurity capabilities, only 34% of Energy, Mining & Utilities respondents feel the same.

Respondents identify the increasing number of cyberattacks as their number-one cybersecurity challenge over the past few years, with the rapid pace of technological innovation and various staffing-related issues following close behind.

Only 2% of respondents said C-level executives had ultimate responsibility for cybersecurity concerns at their organizations, and 1 out of 6 does not have a dedicated in-house cybersecurity response team.

Only around half of survey respondents overall (51%) possess dedicated cybersecurity insurance.

Just over half of all respondents (53%) do not currently have a policy in place for responding to ransomware attacks.

As far as consequences of cyber incidents are concerned, respondents are most worried about data leaks (27% of first-place votes), direct financial losses (20%), and potential fines (19%).

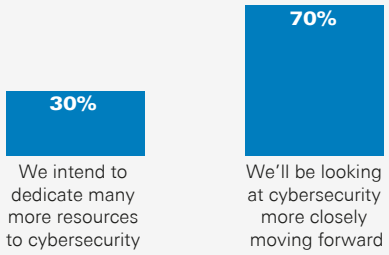
UNCHARTED TERRITORY

Businesses are having to fortify themselves against a growing array of attack vectors. Cyber risk mitigation is mission-critical for preventing not only financial losses, but also brand damage and heavy fines from regulators. And while a clear majority of respondents (63%) in our research agree that cybersecurity is essential to their organization, including 32% who strongly agree, there is a notable delineation between sectors.

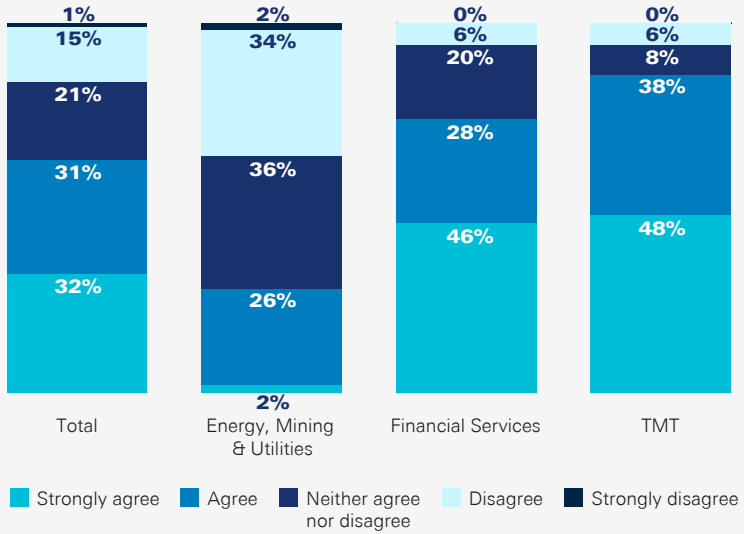
In the lead are TMT executives (86%), followed by their financial services peers (74%), who are clearly in agreement over the importance of their organizations' security measures. Trailing far behind is the EMU sector, with more than a third (36%) of respondents from the industry neither agreeing nor disagreeing that cyber risk measures are essential, and as many in fact disagreeing with that assertion.

However, even among the 16% minority across all sectors who disagree that cyber risk mitigation is critical for their organization, with that subset made up largely of EMU respondents, a full 70% concede that they will be looking at cybersecurity more closely moving forward.

If "Neither agree nor disagree," "Disagree" or "Strongly disagree," do you expect cybersecurity to become a priority for your organization in the near term?



To what extent would you agree with the following statement: 'Cybersecurity and cyber risk mitigation are essential to our organization'?



Despite almost half of respondents having suffered a cyber breach serious enough to require notification of regulators and/or affected individuals, **67% claim confidence** in their organization's ability to detect and mitigate a breach.

Cost Conscious

Companies must think carefully about their cybersecurity budgeting. There is no one-size-fits-all approach. One thing, though, is clear—spending is rising. It has been estimated that expenditure on cyber defenses and risk mitigation totaled $150 billion in 2021, an increase of 12% from the year before, according to Gartner figures. This is expected to rise further in 2022 in lockstep with the volume of threats and as providers hike their fees amid ongoing inflation.

"Protecting their company and its assets from a major cyberattack is the number one thing on every board member's mind," says Justin Hovey, Pillsbury's Technology Industry Group leader.

Organizations spending less than 5% of their technology/IT budget on cybersecurity are in the absolute minority. Our research shows that just under half (49%) are allotting between 6%-10% of this budget for these purposes, and 41% are directing upwards of 10% to security measures.

Organizations in the financial services and TMT sectors are the biggest allocators, which speaks to the nature of their most valuable assets being data. Over half (52%) of banks and other financial firms say they direct upwards of 10% of their IT budgets towards fortifying their cybersecurity, and 48% of TMT firms say the same. Just 24% of executives from EMU companies are taking the same budgetary measures.

Target-Rich Environs

Cybersecurity can often feel like a game of Whack-A-Mole. For every threat vector that is fended off, another mode of attack arises. Criminals continue to develop new ways of infiltrating organizations, while the volume of intrusions is on an ongoing upward trajectory. The FBI's Internet Crime Complaint Center, for example, reported 847,376 complaints of suspected cybercrime in 2021, a 7% rise from the year before.

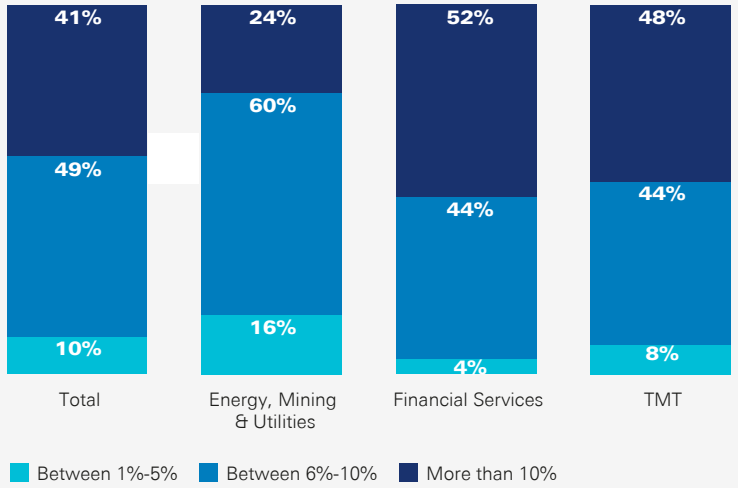
In our survey a quarter of respondents, the largest share, report that the number one cybersecurity challenge their organization has contended with over the past few years has been the rising rate of cyberattacks. "The increasing volume of attacks is higher than we were anticipating," says the CEO of a U.S. EMU company. "The DDoS attacks are also increasing, and sometimes we cannot find the source of the attack on time. It can disrupt our entire operation. We are concerned about the long-term effects on our reputation."

It is a never-ending competition between malevolent actors and their targets, especially as businesses continue to digitalize their operations. Gartner estimates that as much as 91% of businesses are currently engaged in some sort of digital initiative. This is by no means isolated to digital-native sectors like TMT or financial services and means businesses across industries must take cyber risk seriously.

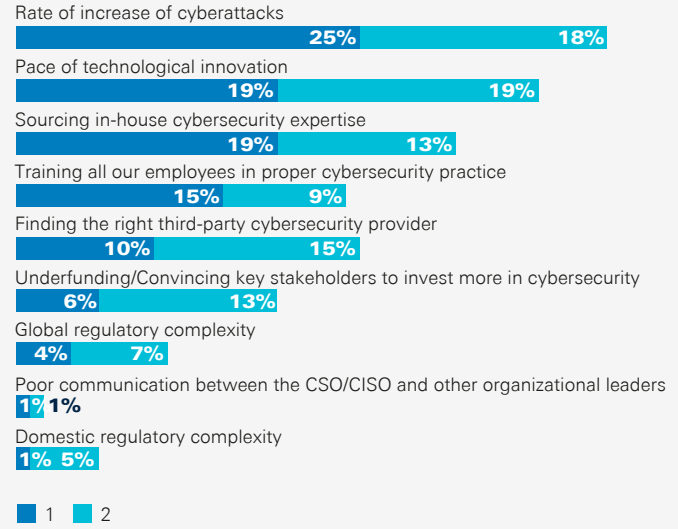
"Given the amount of data-driven decision-making processes, there is a lot of data on the cloud and also on traditional storage systems. Cyberattacks are targeting all types of systems," says the CFO of a U.S.-based TMT company.

This pace of technological innovation, both among companies and their assailants, is seen by 19% of our survey respondents as the top cybersecurity challenge. In joint second place also with 19% of the vote is the difficulty firms experience in sourcing adequate in-house cyber expertise, as companies clamor for limited supply. The two clearly go hand-in-hand. Without the requisite expertise available to the organization, it is impossible to embed the best technical defenses.

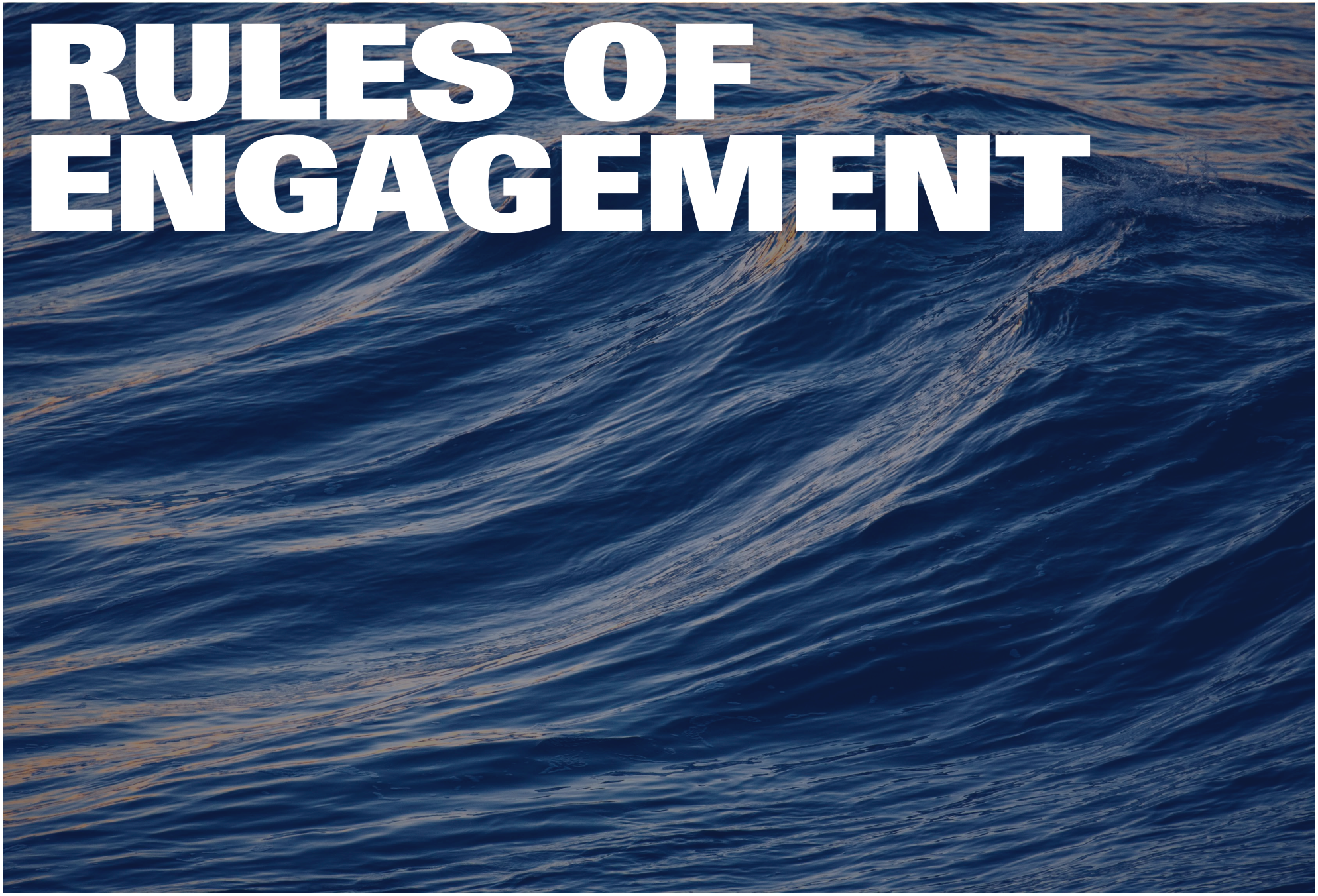
Approximately how much of your organization's technology/IT budget is allocated to cybersecurity-related matters?



What has been the biggest cybersecurity-related challenge that your organization has faced in the past few years?
Rank 1-2, where 1=biggest challenge



RULES OF ENGAGEMENT



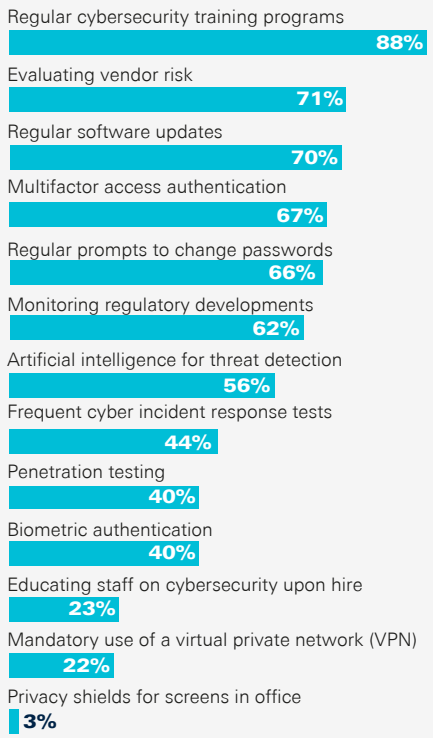
As challenging as managing cybersecurity risk may be, respondents are on balance confident about the measures they are currently taking. Two-thirds (67%) are optimistic about the ability of their organization's existing cybersecurity capabilities to detect and mitigate attacks, including 17% who say they are very confident. TMT and financial services executives express the most confidence, with EMU again trailing. A full 86% of TMT respondents and 80% of in financial services executives are confident in their current systems, whereas just 34% of those in the EMU space hold this view.

Bracing an organization against intrusions can be narrowed down to two approaches: technological and human. Companies can install the strongest firewalls and malware protections available, but all it takes is one employee to click on a malicious link to incur severe damage. This is why education initiatives are so important, and even more so in the wake of the pandemic.

As the in-house counsel of a Swiss EMU company observes: "Bad actors are taking advantage of remote working, so companies need to upgrade their defenses. They also need more time to educate their employees on how to comply with the data protection norms," they say. "There are opportunities for cybersecurity companies to develop solutions relevant to remote working in particular."

The most common policies that respondents employ to mitigate security risks include regular cybersecurity training programs (cited by 88%), evaluating vendor risk (71%), and regular software updates (70%). Several other procedures or technologies are cited by a majority of respondents, of which the most cutting-edge is the use of artificial intelligence (AI) for threat detection (56%).

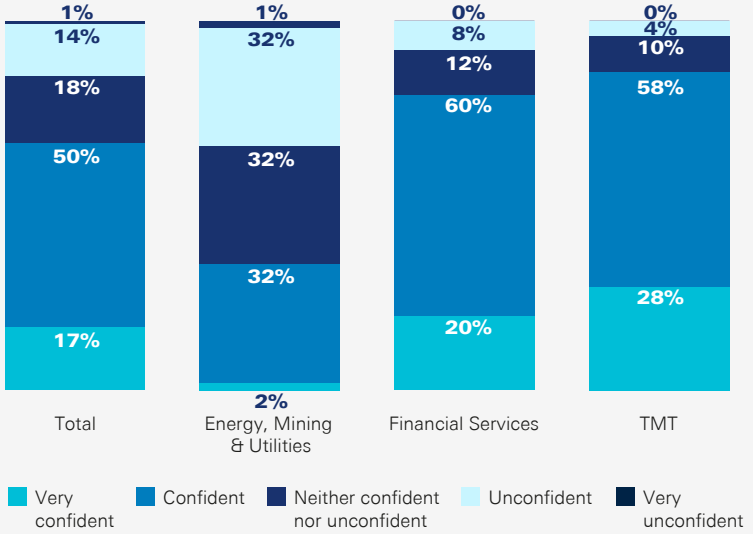
Which of the following technologies or policies do you currently employ to mitigate security risks?



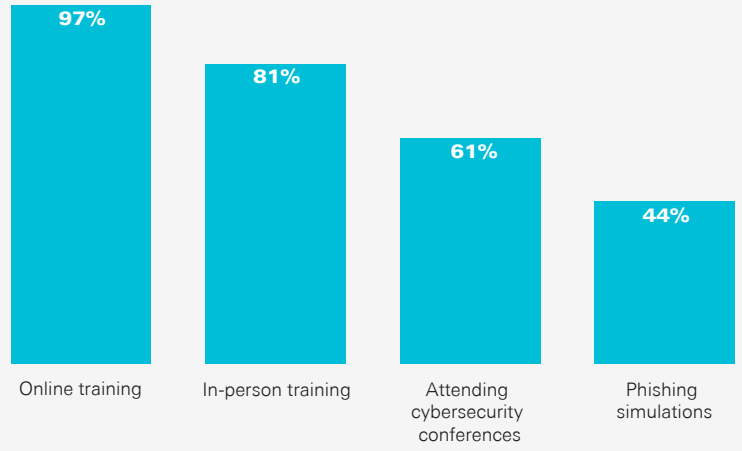
Continuous Learning

Employee training is the bedrock for any successful cybersecurity program, and our survey respondents recognize this fact. Almost all (97%) provide online training to their employees, and 81% say they give in-person training. These efforts are not in vain either, although there is room for progress. Overall, 54% of respondents are either confident or very confident that all of their organization's employees know the

How confident are you in the ability of your organization's existing cybersecurity capabilities to detect and mitigate cyberattacks?

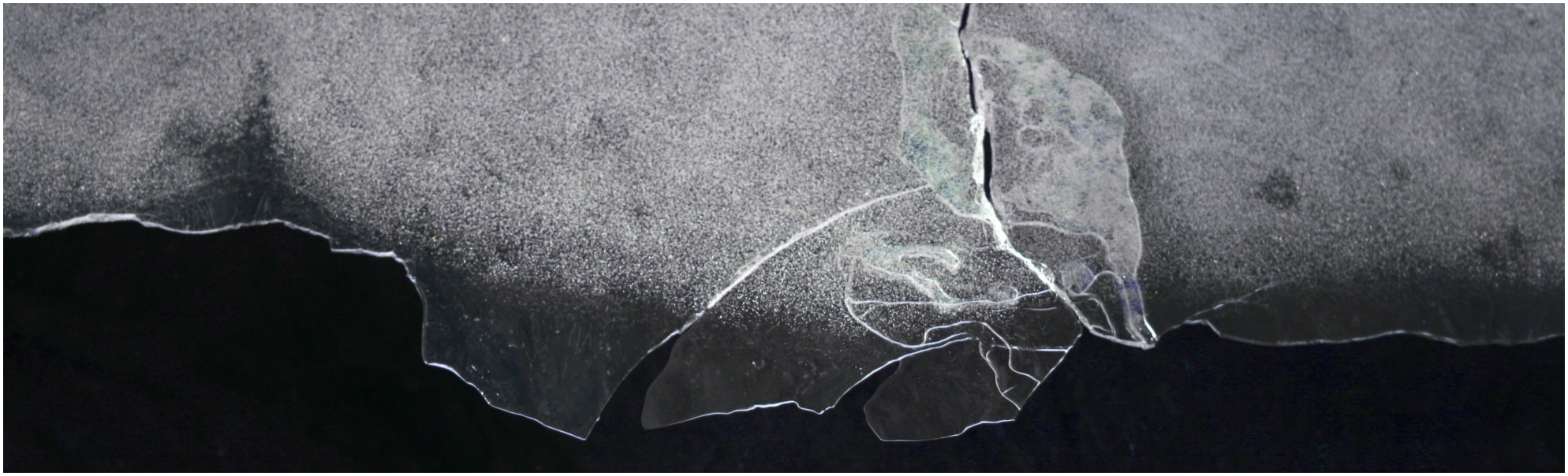


What forms of cybersecurity education or testing does your organization undertake to train employees?



"Organizations are facing increasing challenges to mitigate cyber risk and to take more proactive and less reactive measures to secure their environments. **You can't fix what you can't measure, though.** Trusted, real-time security ratings, just like credit ratings, are now a must-have for organizations to achieve greater visibility across their own entire attack surface and to measure and continuously monitor third-party suppliers."

Dr. Aleksandr Yampolskiy
CEO and Founder of SecurityScorecard



best course of action when confronted with signs of cyber risk or a cyberattack.

Specifically, 68% of respondents from the financial services sector and 70% of their TMT peers are either confident or very confident on this point, whereas only 26% of EMU respondents report the same. However, that does leave 45% across all sectors who admit that they are neither confident nor unconfident or who are outright unconfident (15%) in their employees' ability to appropriately respond to cyberattacks. This awareness gap will need to be closed for those falling behind.

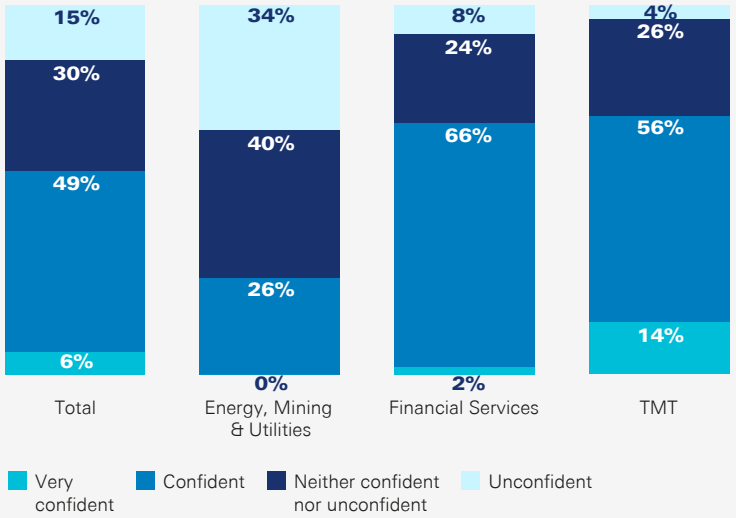
"Financial institutions often feel confident in their current cybersecurity infrastructure," says Deb Thoren-Peden, co-leader of Pillsbury's Cybersecurity, Data Protection & Privacy and Fintech, Payments & Blockchain teams. "But with the stakes so high for those types of organizations, they must constantly ask themselves, 'What happens when there is a breach?'"

A major challenge in keeping staff up to speed is the pace with which the natures of cyber threats change, which can cause programs to become outdated quickly. Companies must be cognizant of this and constantly update their content and be attentive to knowledge gaps. "Even the training given a year ago would not prepare teams enough to protect systems and mitigate today's risks," admits the CISO of a U.S.-based EMU company. "We have to keep them informed about the latest attacks and the methods cyber criminals employ."

Building Barricades

Beyond the basics of education and raising cyber awareness among staff, there are of course more technical ways in which organizations are protecting themselves. The most popular means of defense, cited by 71% of respondents, is adopting behavior analytics. This is a technique that involves monitoring networks to detect anomalous user behavior and identify any potential insider malfeasance.

How confident are you that all employees in your organization know the best course of action when confronted with signs of cyber risk or a cyberattack?



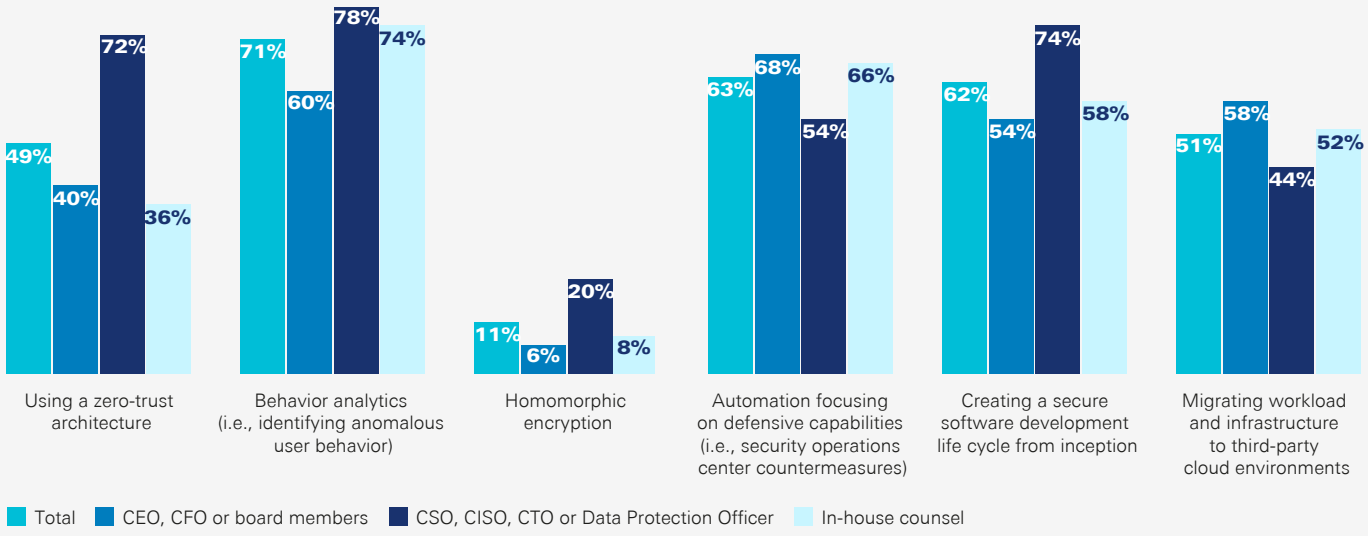
Survey respondents in data- and security-centric roles, such as CSOs, CISOs and CTOs, take a more foundational, from-the-ground-up view. For example, 74% underscore the importance of creating a secure software development life cycle from inception, and almost as many (72%) point to the value of building the network on zero-trust architecture. Zero-trust models require more than simple user authentication, adding a layer of verification at the device level and are becoming increasingly common.

By contrast, respondents in more traditional C-suite positions, including CEOs, CFOs and board members, emphasize the value of automated defensive capabilities (68%) and migrating workloads and infrastructure to third-party cloud environments (58%). The latter includes services such as Google Cloud Platform and AWS, which benefit from the advanced expertise and security investments made by their respective parents, Google and Amazon.

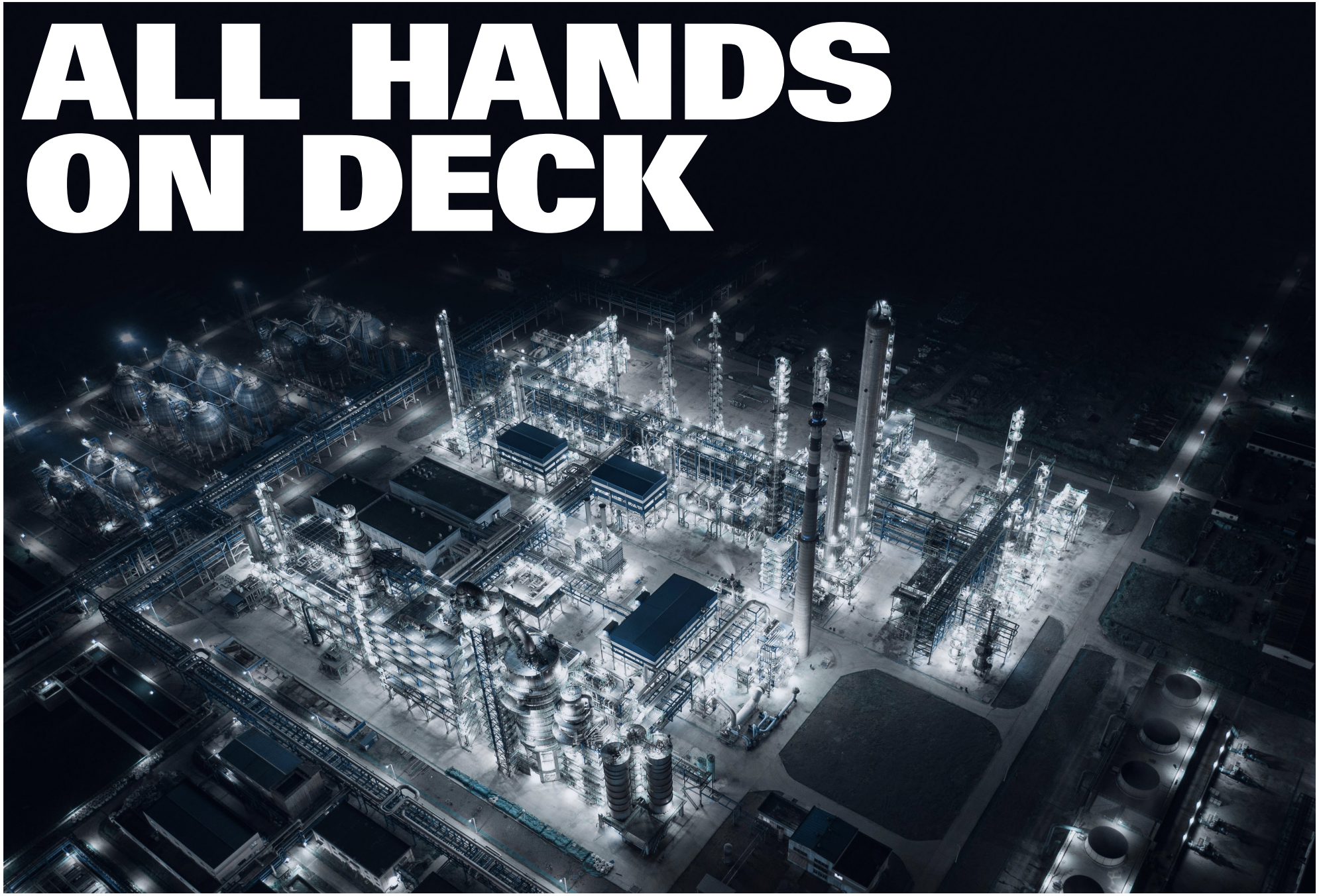
45%

Share of respondents who say they are less than confident employees within their organization know the best course of action when confronted with signs of a cyberattack.

How are you planning to mitigate cybersecurity risks?



ALL HANDS ON DECK



A business is nothing without valid, well-founded cyber governance standards in place. This should be a codified framework for how the organization controls its cybersecurity risk, including delegation of accountability and decision-making, from the very top level down to the more practical and technical aspects in the IT or technology function. This model should be followed unswervingly to avoid any governance drift, which can lead to a breakdown of risk accountability and clearly delineated roles.

Regarding the highest level of oversight of cyber risk, it is somewhat surprising that just 2% of respondents reported that C-Suite executives have ultimate responsibility given the stakes. Responsibility most often falls either to a risk committee, according to 48% of our respondents, or the board, cited by 43%. In terms of individual responsibility for organizations' cybersecurity concerns, meanwhile, this is mostly the domain of a head of department or senior vice president, per 57% of respondents, otherwise general counsel takes up the mantle (41%).

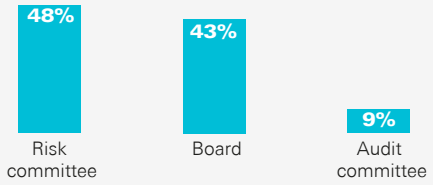
In-House Insights

Businesses have to respond to cyber incidents swiftly and decisively. In the vast majority of cases this need has seen them equip themselves with dedicated in-house cyber incident response teams.

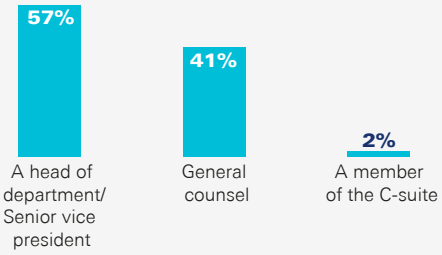
The key benefit of this approach is responsiveness. The difference between a threat being rapidly detected after intrusion and dispatched versus bad actors having ample time to act can amount to tens, if not hundreds, of millions of dollars.

That response advantage comes with its own financial cost, however, and for this reason some organizations take a more generic approach. "Our IT department currently plans and manages the incident response strategies," says the CEO of a U.S.-based EMU company. "We have not set aside funds for a dedicated unit so far."

Does your organization's board or a committee of the board have oversight of cybersecurity risk?

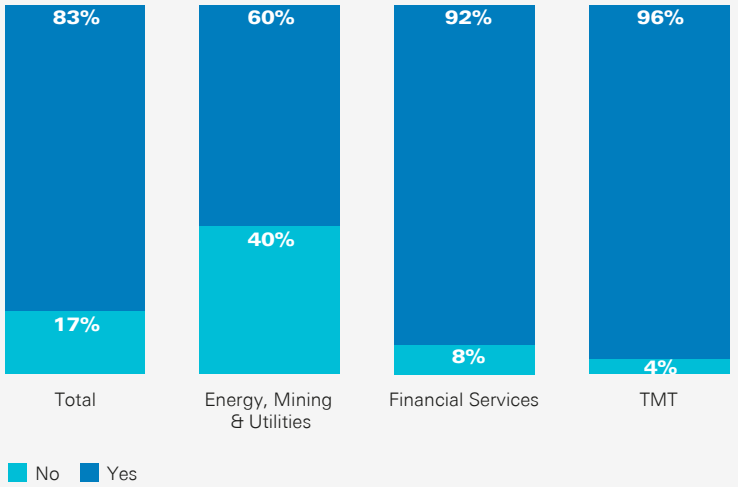


What senior executive in your organization has ultimate responsibility for your cybersecurity concerns?

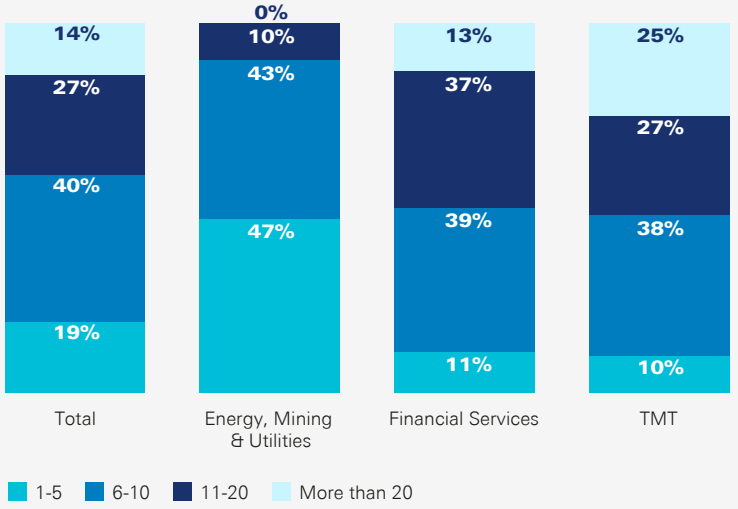


Encouragingly, these cases are in the minority. As much as 83% of respondents report having a dedicated in-house incident response team in place. TMT and financial services businesses are far more likely to report having these resources under their roofs, at rates of 96% and 92%, respectively, with EMU organizations once again lagging. Even then, 60% of these companies directly employ a cyber response team, although they tend to be smaller. Our research shows that 47% of EMU companies' response teams consist of just 1-5 people, whereas respondents in the financial services and TMT sectors mostly have teams with headcounts well in excess of this.

Does your organization have a dedicated in-house team with full-time responsibility for cybersecurity/cyber incident response?



If your organization does have an in-house team, how many people are a part of that team?



When those who lack dedicated response resources were asked what approach they take instead, they generally responded that this is the domain of their IT departments. In such cases, it's paramount that, at the very least, these more generic functions have direct cybersecurity expertise within them.

Striking a Balance

Outsourcing versus keeping activities in-house is a perennial question for businesses and across all their operations, with cybersecurity being no exception. On balance, organizations are keeping this close to home, with 40% of our survey respondents saying they keep their cyber functions mostly in-house and 2% saying it is exclusively self-managed.

This is particularly true of incident response activities, which comes back to the key issue of being quick to react to threats. "We need to be certain that the response time is kept to the minimum," says the counsel of a U.S.-based TMT company with a cybersecurity team of 20 people. "External providers will not be able to manage incidents with appropriate priority. They might have other clients dealing with the same issues and we would be left fending with the resources we do have."

A third of respondents say these cyber functions are balanced equally between in-house teams and outsourced partners. The maturity of cyber risk management correlates with these outsourcing trends, as demonstrated by the differential between sectors. Almost half (46%) of EMU respondents say they mostly outsource their cybersecurity functions to a third party. Only 14% of both TMT and financial services executives surveyed report the same.

Instead, financial services respondents are more likely to strike an equal balance between internal and external teams (44%) or keep things mostly in-house (42%). TMT companies are even more likely to keep things mostly (54%) or entirely (2%) in-house.

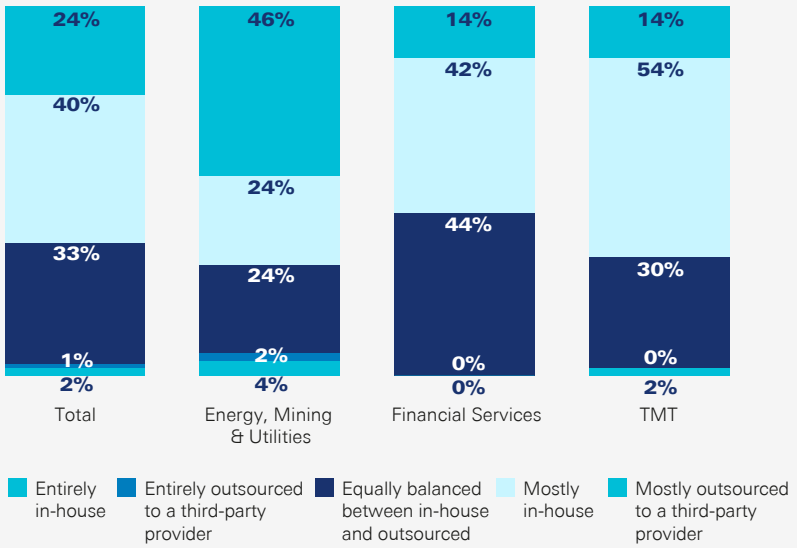
Of the 26% of respondents overall who say they mostly or entirely outsource cybersecurity functions, all require their third-party vendors to give immediate notice in the event of a breach, emphasizing the primacy of response times. A further 84% ask that they have a designated disaster recovery plan in place, among other requirements.

"In many cases, it will be mandatory for a business to appoint a dedicated 'data protection officer' (DPO) as part of their cyber governance framework, with defined statutory roles," says Steven Farmer, a partner in Pillsbury's Technology Transactions, Data Privacy and International Trade teams. "DPOs must operate without a conflict of interest within a business, making them essentially a regulator within the business when cyber incidents occur."

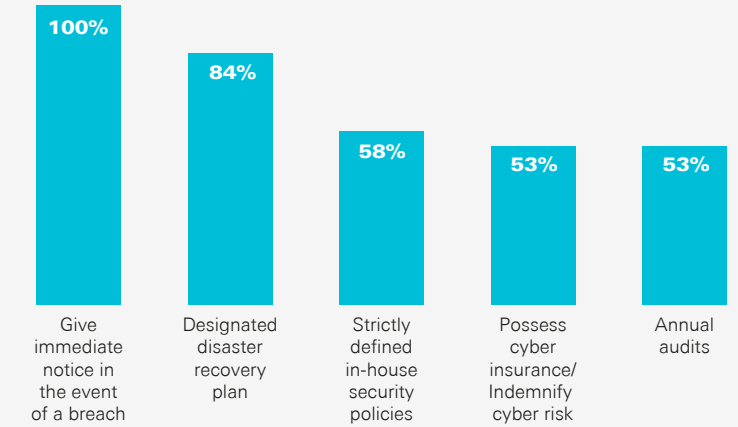
40%

The share of respondents in the energy, mining & utilities sector whose organizations do not currently have a dedicated in-house team with full-time responsibility for cyber incident response.

To what extent are your organization's cybersecurity functions kept in-house or outsourced?



If "Mostly outsourced" or "Entirely outsourced," what policies does your organization require third-party vendors to possess?



ENEMY AT THE GATES

Staying on top of changes in the legal and regulatory landscape related to cybersecurity and data privacy is a challenge in and of itself. Last year, the Federal Trade Commission (FTC) updated its longstanding safeguards rule to keep pace with current technologies.

The FTC demands that businesses take a risk-based approach by embedding a codified information security program that is appropriate to the size and complexity of the organization, the nature and scope of its activities, and the sensitivity of the data it manages. Specific measures include conducting risk assessments, implementing and monitoring safeguards, staff training, continuously updating the security program, and formalizing incident response plans.

For multinational businesses, staying up to date with these obligations is even more complex. Close to three quarters (71%) of our survey respondents say they have someone on staff who is responsible for tracking these developments, both locally and globally. Although most EMU companies (54%) do employ such an individual, they are less likely to do so than their peers in the TMT (76%) and financial services (84%) sectors.

Rewarding Proactivity

Understanding the external threat and legal environment inevitably requires an internal response. Cybersecurity policies are not static and must account both for the changing nature of the threat and what is required of governments and regulators. The bulk of respondents (39% overall) say their organizations review their cybersecurity policy annually, which includes the majority of EMU respondents surveyed (52%).

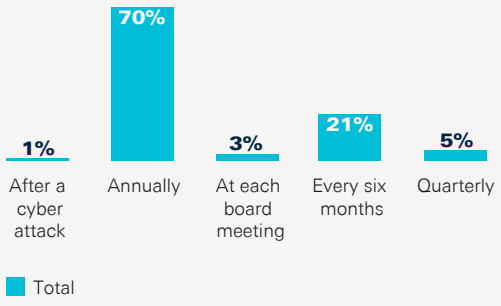
Financial services firms are taking a more proactive approach. The largest share of these respondents (44%) report reviewing their cybersecurity policy every six months, as do just under a third (32%) of TMT respondents. Moreover, sizable minorities from each of these two sectors conduct quarterly reviews (28% and 30% of financial services and TMT companies, respectively).

Regardless of how frequently these reviews are conducted, most respondents (70%) say they present those reviews or other cybersecurity updates to their board on an annual basis. Policy reviews are critical, but there must also be assurance work to confirm that what is documented is actually executed by staff in their day-to-day workings.

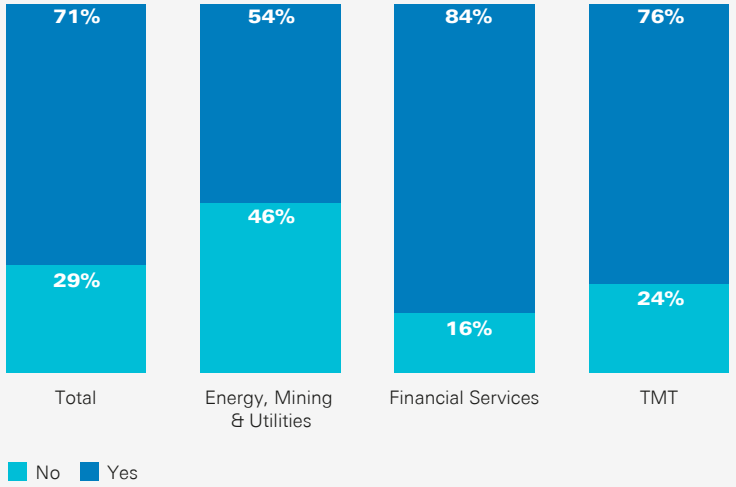
A policy is worthless if it is not actively followed, as the in-house counsel of a U.S.-based TMT company stresses: "Our teams conduct cybersecurity policy reviews annually. It is important to ensure that these policies are practiced, too. Once they are rolled out, we update our staff and other relevant stakeholders so that they can implement them."

Cyber policies needn't be overcomplicated but should be revisited and updated as regularly as is feasible to reflect the rapid emergence of new threats and legal obligations. "We like to take a very proactive approach

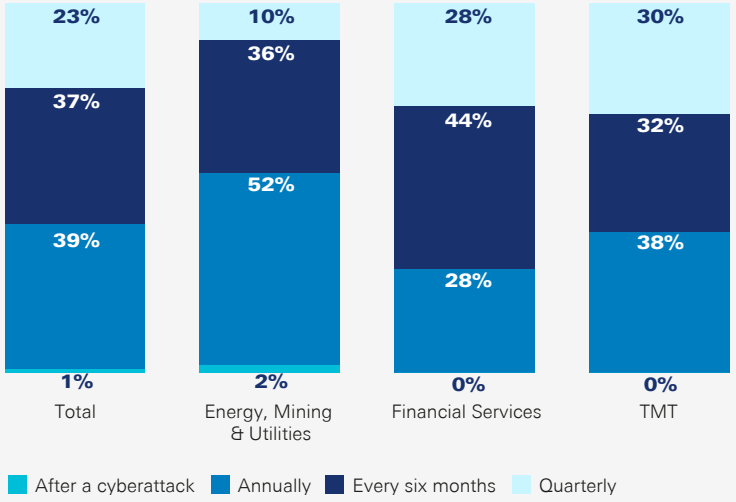
How frequently are those reviews or other cybersecurity updates presented to the board?



Does your organization have someone on staff with responsibility for tracking legal developments, both locally and globally, related to cybersecurity and data privacy?



How frequently does your organization review its cybersecurity policy?
Rank 1-2, where 1=biggest challenge



Despite the speed and complexity of cybersecurity and data privacy regulation, 1 in 3 respondents say **they do not have someone on staff** actively tracking related legal developments.

when it comes to cybersecurity. Reviewing the policy documents and ascertaining changes on time is vital," says the chief privacy officer of a U.S. financial services company that reviews its cybersecurity policy quarterly, adding that company rules can be as simple as changing passwords or using and avoiding specific platforms while at work.

Under Cover

Cyber liability insurance is increasingly common. This coverage protects businesses against income losses and recovery costs, such as data restoration and re-securing networks. Such insurance has become even more pertinent since the advent of the European Union's General Data Protection Regulation (GDPR), which carries hefty fines for data breaches.

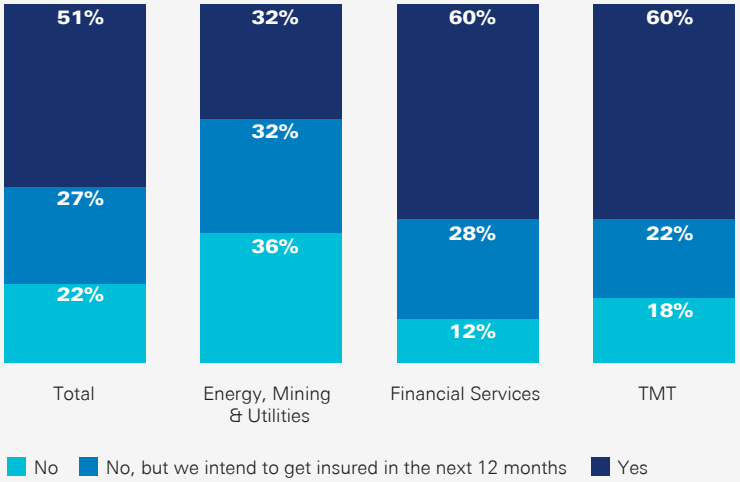
The regulation, which applies to any business dealing with European citizens' personal data, regardless of where the organization is headquartered, can see companies face fines of up to $10 million or an excruciating 2% of an entire group's global turnover, whichever is higher. Therefore, having appropriate coverage in place can be an important part of a company's protections against cyber risk.

"Cyber insurance covers 'gaps' in companies' traditional insurance programs," advises Tamara Bruno, partner in Pillsbury's Insurance Recovery & Advisory Practice. "It is crucial for companies to identify those gaps, determine whether they can take on such cyber risks or effectively shift them to contract parties, and evaluate how cyber insurance may help protect them at least against larger cyber losses."

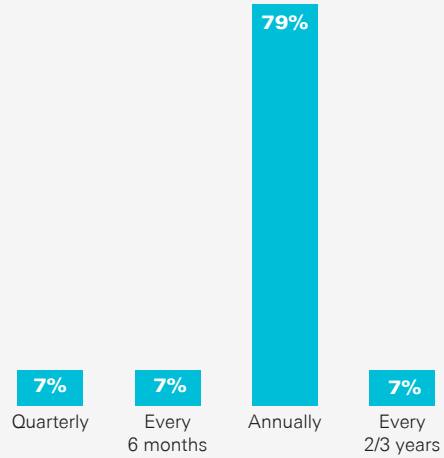
Most organizations (51%) do possess dedicated cybersecurity insurance, and a further 27% say they intend to put a policy in place over the next 12 months. Financial services and TMT companies are much more likely to have invested in these policies (both 60%) than EMU companies (just 32%). In fact, more than a third (36%) of EMU companies surveyed say they don't have any such insurance.

Of the 51% of respondents across all sectors who do already possess dedicated cybersecurity insurance, an overwhelming majority of 79% say they review the terms of the agreement annually. Business operations are always changing and therefore, just like any other form of corporate insurance, cyber policies must be reviewed at least annually to confirm that there are no gaps and whether any supplemental coverage is required. "Insurers continue to change their cyber policy terms in response to developments in cyber risks," Bruno notes. "Work with your broker and insurance counsel on negotiating terms to fit your operations."

Does your organization currently have dedicated cybersecurity insurance?



If your organization does have cybersecurity insurance, how often does it review the terms of the agreement?



> "Cyber insurance covers 'gaps' in companies' traditional insurance programs. It is crucial for companies to those identify gaps... and evaluate how cyber insurance may help protect them at least against larger cyber losses."
>
> **Tamara D. Bruno**
> Insurance Recovery & Advisory partner

U.S. Cybersecurity Law

Russia's war in Ukraine prompted the U.S. government to take legislative action on cybersecurity this year. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) was signed into law by President Biden in March as part of the Strengthening American Cybersecurity Act. CIRCIA requires the Cybersecurity and Infrastructure Security Agency (CISA) to develop and implement regulations requiring covered entities to report covered cyber incidents and ransomware payments to CISA. At the core of this law is the obligation of such entities—including companies in the energy, defense, financial services, chemicals production, and health care sectors, among others—to report within 72 hours any major cyber incidents. This is regardless of whether these events result in data breaches.

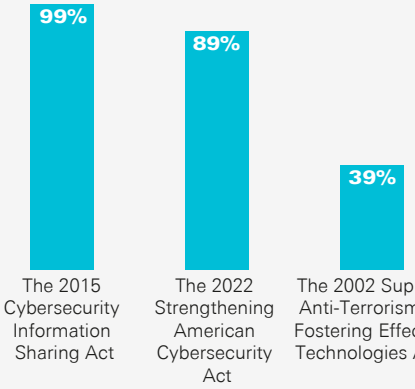
"The federal government, for better or worse, has jumped with both feet into cybersecurity regulations," says Brian Finch, a Pillsbury Public Policy partner and recognized authority on global security and cybersecurity threats. "Between CIRCIA, the regulation of pipeline cybersecurity through the Transportation Security Administration, and other measures, every company in the United States should expect to have some sort of cybersecurity control imposed on it by virtue of U.S. federal law."

It is the latest addition to the federal toolkit, following the introduction of the 2015 Cybersecurity Information Sharing Act, which made it easier for companies to share personal information with the government, especially as it relates to cyber threats. Practically all U.S.-based respondents (99%) in our research are personally aware of the 2015 Cybersecurity Information Sharing Act, and 89% are aware of the 2022 Strengthening American Cybersecurity Act.

However, they are far less familiar with the cybersecurity-related provisions in the 2002 SAFETY Act, with only 39% reporting an understanding of these elements of this piece of legislation. The act ensured liability provisions for cybersecurity firms such as makers of anti-virus programs, firewalls, mobile security systems and mobile applications, whose products may be used by terrorists or criminals to carry out attacks.

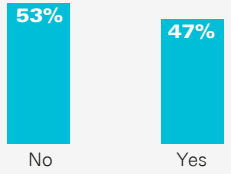
Of the minority of U.S. respondents who are aware of the 2002 SAFETY Act, just over half (53%) have not yet applied for or considered applying for

Which of the following pieces of U.S. legislation are you personally aware of?

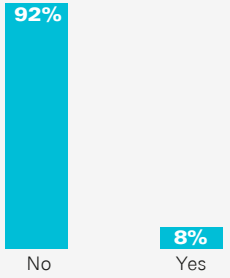


*(a.k.a. the SAFETY Act, whose liability protections apply to a wide range of anti-terrorism products, systems, and services)

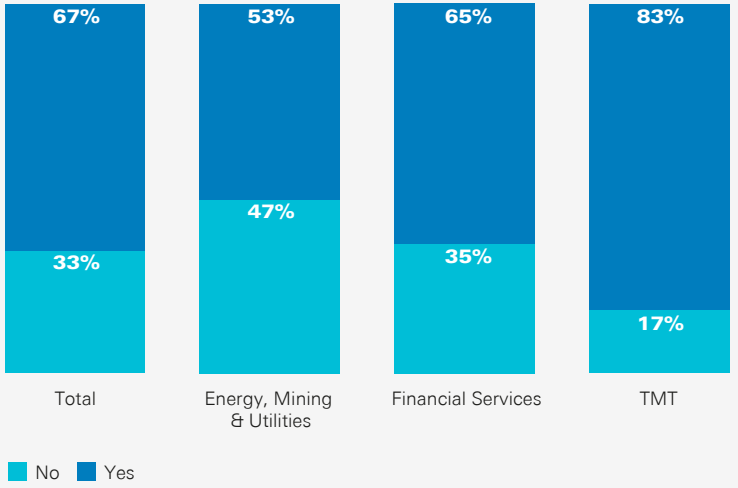
If "SAFETY Act" was selected, has your organization applied for or considered applying under the U.S. SAFETY Act?



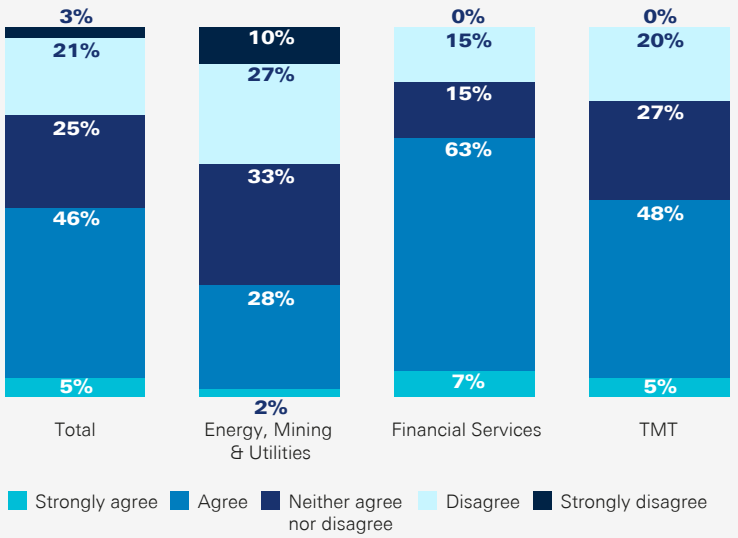
To date, have you made use of any of the protections provided by the state under those pieces of legislation?



Do you require third-party vendors to take advantage of liability safe harbor laws, such as the U.S. SAFETY Act?



To what extent would you agree with the following statement: "The guidance provided by the government and local regulators on cybersecurity is suitably helpful and sufficient for our organization's requirements."



protections under the law. Only 8% of respondents say they have made use of any of the protections provided under this piece of legislation.

That said, just over two-thirds (67%) of U.S.-based respondents require their third-party vendors to make use of liability safe harbor laws, such as those provided in the 2002 SAFETY Act. For those that don't, the main reason given seems to be a reluctance to abdicate this responsibility to third parties. For example, the chief information officer of a U.S. TMT company, says: "There could be many underlying risks of allowing third parties to manage the procedures of seeking these protections. The claim may be held invalid if third parties do not present the facts well."

Generally speaking, across both the legislative and regulatory spectrums, respondents are mostly positive about the guidance that public bodies and agencies make available to them. Just over half of U.S.-based respondents agree that the guidance provided by the government and local regulators on cybersecurity is "suitably helpful and sufficient for their organization's requirements," leaving 25% who are indifferent to this statement and 24% who disagree. So far, public bodies appear to be doing a solid job of keeping organizations up to speed.

"The federal government, for better or worse, has jumped with both feet into cybersecurity regulations... Every company in the U.S. should expect to have some sort of cybersecurity control imposed on it by virtue of federal law."

Brian Finch
Pillsbury Public Policy partner

THE AFTERMATH

It is not just data regulators operating under the auspices of the GDPR and similar data laws that are keeping company executives up at night—there are also civil legal actions to consider. In July 2022, an SEC filing showed that telecommunications giant T-Mobile was paying an aggregate $350 million to settle a consolidated class action lawsuit after the information of 77m customers was found for sale on the dark web. The company also committed to investing $150 million in updating its data security and technology in 2022 and 2023 to prevent a repeat breach.

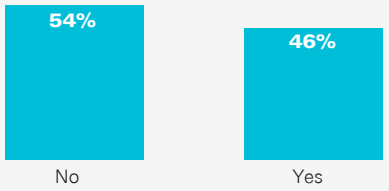
In many instances, companies are legally obliged to disclose intrusions and data breaches. However, this will often depend on whether personal data was leaked as a consequence of a hack. Given the choice, some companies will choose to address a cyberattack entirely internally to save face.

"Following an important 2022 development before the Court of Justice of the EU, consumer protection associations can now raise class action-style lawsuits on behalf of individuals whose data is breached without first needing their consent to do so, paving the way for a deluge of EU based litigation where cyberattacks occur," Pillsbury's Farmer adds.

How organizations participating in this survey respond to attacks varies widely according to the sector in which they operate. For instance, the vast majority (78%) of EMU respondents report that their cyber leaders never share information about cyberattacks. In comparison, TMT and financial services respondents come across as much more communicative, with only 34% and 22% from these sectors, respectively, reporting a similarly closed-book approach. Especially in the latter's case, their cyber leaders mostly share information about attacks voluntarily and transparently (52%).

According to most respondents (51%), the single best way to incentivize the voluntary reporting of cyber incidents is to provide the discloser with legal protections against lawsuits. A third of respondents believe the best course of action is simply to make this information a requisite element of formalized disclosure agreements, prompting people to speak up. Meanwhile, regarding mandatory reporting, a large minority of respondents (46%) say they have suffered a cyber breach or security incident that required them to notify government regulators or individuals whose data may have been compromised.

Has your organization suffered a cyber breach or security incident that has required a notification to government regulators or any individuals whose data has been compromised by the breach?

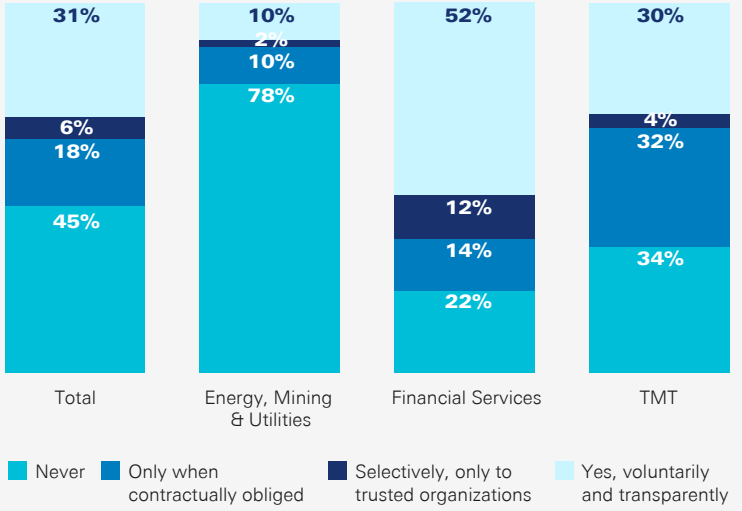


Enemy at the Gates

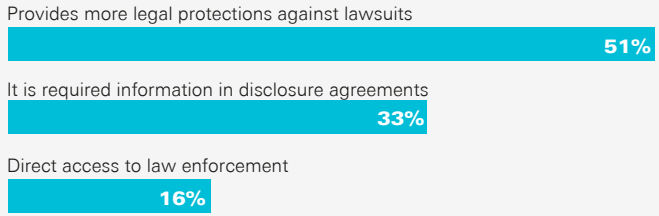
According to our respondents, the most common type of cyber attacker is hacktivists, which 98% of those who share information on attacks say they have been targeted by. Almost two-thirds (65%) reveal that they have been the target of insider threats, whereas just 11% overall have been targeted by state-sponsored attackers.

Regarding the latter point, respondents in the TMT sector in particular report a higher detection of state-sponsored attackers. Over a quarter of these survey participants report this, versus just 10% of financial services respondents and 0% of EMU respondents.

Do your organization's cyber leaders share information about cyberattacks?

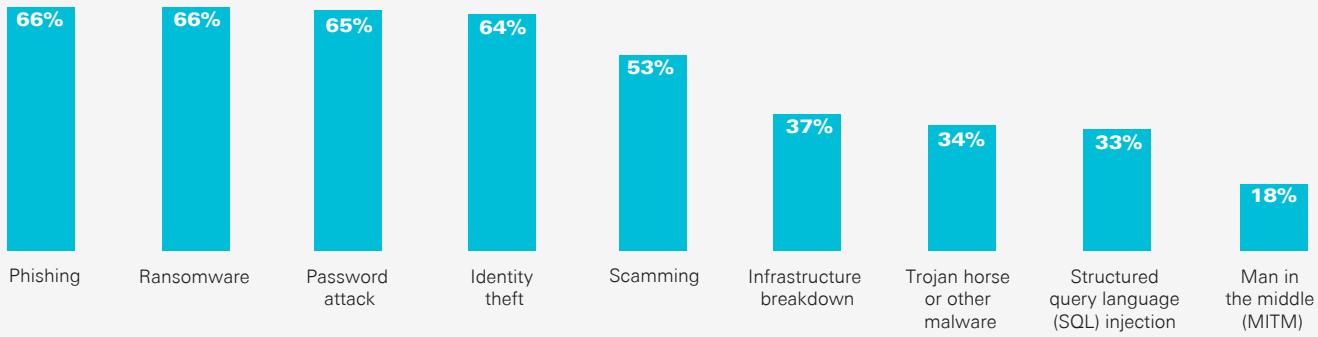


What do you consider to be the biggest incentive for voluntary disclosure of cyber incidents?

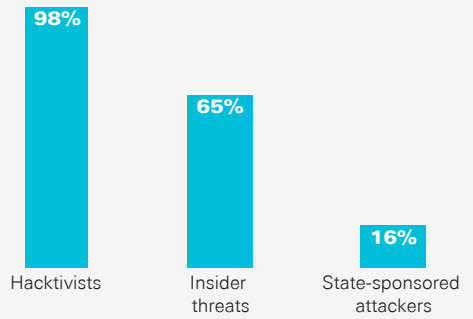


A clear indication that information is more valuable than ever, **nearly half** (46%) of respondents see data leaks as representing one of the two biggest potential consequences of a cyberbreach, surpassing even direct financial losses (42%).

To the best of your knowledge, which of the following types of cybersecurity attack have targeted your organization?



To the best of your knowledge, which of the following types of cyberattackers have targeted your organization?



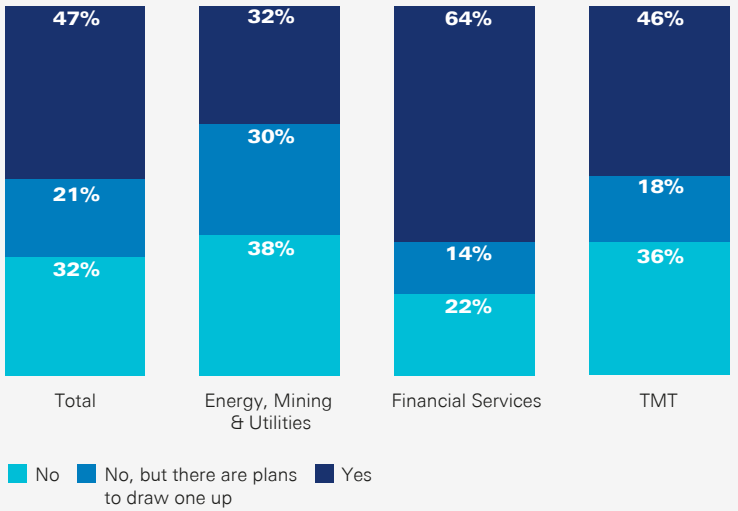
Technology has become a clear point of contention in national security considerations and there are countless examples of state actors exploiting software companies and social media platforms to sow disruption. However, the zero response from EMU respondents may belie a lack of cyber intrusion detection capabilities rather than a lack of threat activity. To be sure, critical energy infrastructure assets are a key target for state actors, and especially during a period of heightened diplomatic tensions, war in Europe, and energy price volatility that is disrupting operators.

Regarding the specific types of incidents that companies have been subjected to, two-thirds of respondents reveal that their organization has suffered phishing attacks, and as many say the same about ransomware attacks. Almost as common are password attacks (65%) and incidences of identity theft (64%). At the other end of the spectrum, only 11% say they have been targeted by a DoS/DDoS attack. This illustrates how most events are motivated by money. While DDoS attacks can take a company offline, they don't infect computer networks or involve data being stolen or access being denied. Phishing and ransomware attacks, by contrast, are almost always perpetrated by criminals seeking financial gain.

It is becoming increasingly common for organizations formalize a ransomware policy as part of their wider cybersecurity protocols. There are essentially two options. Either meet the attackers' demands and hope they back off, claiming against an insurance policy where possible. Otherwise, refuse to pay and face the consequences. Overall, just under half of respondents (47%) have a policy in place for responding to ransomware attacks, and a further 21% say they have plans to draw one up.

Organizations in the financial services sector are in the lead on this, with 64% already having a policy in place. Roughly equal shares of respondents in the EMU (38%) and TMT (36%) sectors divulge that they currently have no such plan in place. And for those with a policy, the protocol for the vast majority (73%) is never to pay. A minority (17%) are prepared to pay, but only if the ransom is covered by their cybersecurity insurance.

Does your organization have a policy in place for responding to ransomware attacks?



Plugging Leaks

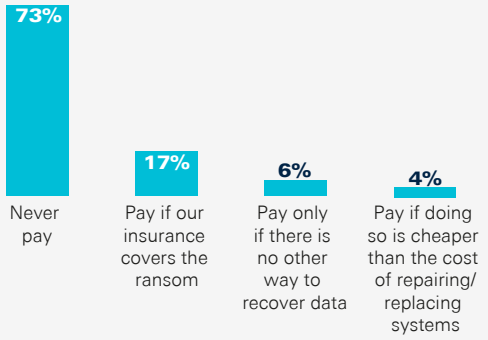
The consequences of cyberattacks stretch far and wide. There is the initial impact of lost income from downtime. In high-profile incidents this can be compounded by brand damage as customers lose trust in a company's ability to store and protect their confidential information, taking their business to competitors. The introduction of punitive regulatory fines has added another layer to consider.

In reality, these consequences are not mutually exclusive but closely related, and in many cases causal. "Data leaks are concerning for us because they could result in direct and indirect financial losses. Data taken from our systems could be used for forging identities, prompting customers to sue our company. There are endless possible consequences linked to data leaks," says the data protection officer of a French financial services company.

It is these data leaks that respondents are most worried about, earning 27% of first-place votes, followed by direct financial losses (20%) and potential fines (19%). The complexity and interconnectedness of these consequences is what companies must bear in mind. And the best mitigation against these various outcomes is taking the appropriate steps to prevent intrusions and, when they do occur, proactively following established response protocols. Failing to do so can cause lasting damage to both brand and shareholder equity.

"Cyberattacks cause a lot of reputational harm. Information about cyberattacks spreads fast and can cause investors to pull their funding. There are a lot of complexities that can arise from an attack," notes the in-house counsel of a U.S.-based financial services company.

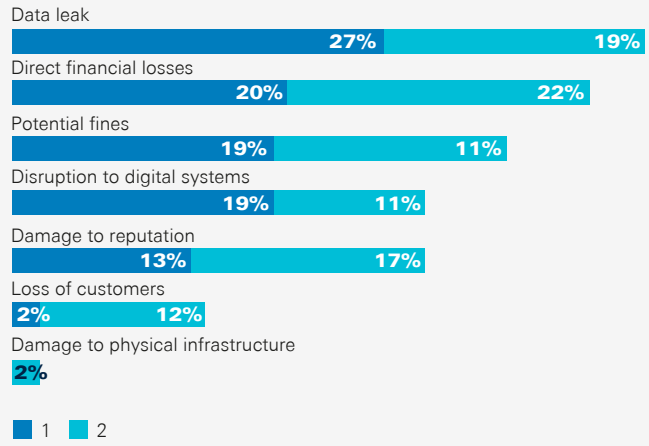
If your organization has cyberattack policies in place, what is your current policy on paying ransoms?



32%

The share of all respondents whose organizations currently have no ransomware policy in place nor have plans to draw one up.

What potential consequences of a cyberattack are most concerning for your organization?
Rank 1-2, where 1=most concerning



OUTLOOK

While acknowledging that the volume of cyberattacks is escalating remarkably quickly, companies overall are confident in their cybersecurity capabilities. Clearly there are some major gaps between sectors, demonstrated by the relative lack of adoption and proficiency of cybersecurity measures in the EMU space.

This should give cause for concern in this highly geopolitically sensitive industry specifically; more broadly, it should prompt dialogue about the efforts needed in other under-guarded yet strategically important areas of the economy. Companies should take their cue from pacesetters in the financial services and TMT sectors, which are well ahead on the cyber maturity curve.

Technology moves fast and with it so does the cat-and-mouse cybersecurity challenge. Reflecting on what will define the coming two years, respondents take a neutral view. On the one hand, 25% of respondents believe the dominant cybersecurity trend will be the development of better tools and processes for threat detection and response. On the other, 21% see the rise of ransomware attacks as the biggest near-term trend. In other words, companies will be able to better equip themselves, but in an increasingly challenging environment.

One major consideration here is the impact that remote working is having on defending the expanded digital perimeters of organizations. A recent McKinsey survey found that 35% of American workers can do their job from home full-time. Another 23% can work from home part-time, and only 13% could work remotely at least some of the time but choose not to.

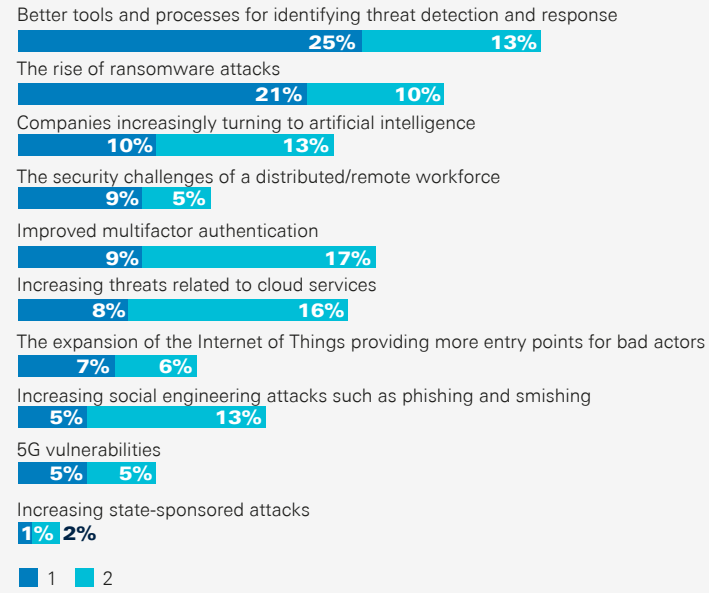
"We already noticed an increase in ransomware cases in the past two years, and that will continue to increase over the next two years," says the chief information officer of a U.S.-based TMT company. "Bad actors have taken advantage of the fact that people are working remotely. They are using the flexibility of the workforce to gain access to company systems."

Bearing the financial costs of cybercriminals holding networks and data to ransom is just one concern. With geopolitical tensions running high, companies will need to exercise caution over the potential for stealth attacks, hackers monitoring systems and surreptitiously stealing data and intellectual property. This rising threat is not only coming from state actors with political motivations.

Industrial espionage is becoming more common and occurring among even modestly sized companies in industries that, unlike defense or energy, are not typically seen as strategically sensitive. In May of this year Virginia-based enterprise software company Appian was awarded $2 billion in damages after Massachusetts competitor Pegasystems was accused of snooping on the company to obtain internal documents.

Such examples will continue to arise and call for companies to continuously improve both their threat detection abilities and the staff training and policies that underpin the more technical measures necessary to keep unwanted attacks at bay. This won't be easy, but it will be more than worth the effort.

What cybersecurity trends do you think will be most important in the next two years?
Rank 1-2, where 1=most important



About Pillsbury

pillsbury

Pillsbury's Cybersecurity, Data Protection & Privacy team helps clients of all sizes and across every industry to proactively manage and safeguard the proprietary information they hold. Bringing together regulatory authorities, litigators, transactional lawyers, intellectual property counsel, seasoned government contracts practitioners and legislative strategists to provide a holistic assessment and response to changing data and cyber landscapes, we help organizations navigate new cyber technologies, adhere to complex and evolving regulations, defend against increasingly sophisticated attacks, and mitigate the financial and reputational harm that can accompany a breach.

For more information, visit **pillsburylaw.com/cyber**.

PILLSBURY CONTRIBUTORS

Tamara D. Bruno | Partner | tamara.bruno@pillsburylaw.com | +1.713.276.7608

Steven Farmer | Partner | steven.farmer@pillsburylaw.com | +44.20.7847.9526

Brian E. Finch | Partner | brian.finch@pillsburylaw.com | +1.202.663.8062

Justin D. Hovey | Partner | justin.hovey@pillsburylaw.com | +1.415.983.6117

Deborah S. Thoren-Peden | Partner | deborah.thorenpeden@pillsburylaw.com | +1.213.488.7320

About Mergermarket

Mergermarket

Mergermarket is an unparalleled, independent mergers & acquisitions (M&A) proprietary intelligence tool. Unlike any other service of its kind, Mergermarket provides a complete overview of the M&A market by offering both a forward-looking intelligence database and a historical deals database, achieving real revenues for Mergermarket clients.

For more information, please contact:

Alissa Rozen | +1.212.500.1394