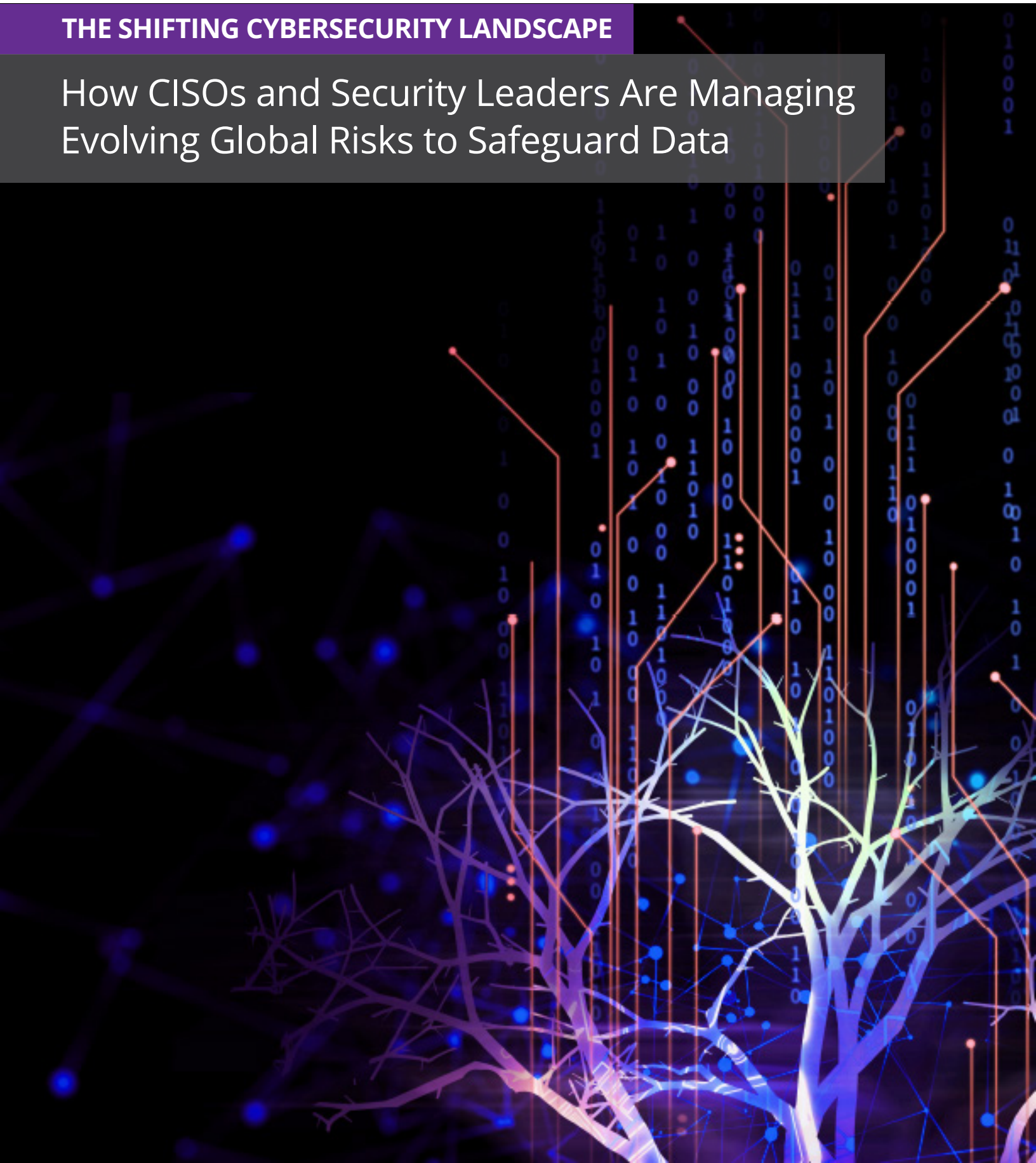
ankura

ARI KAPLAN ADVISORS

THE SHIFTING CYBERSECURITY LANDSCAPE

How CISOs and Security Leaders Are Managing Evolving Global Risks to Safeguard Data



CONTENT

INTRODUCTION

Each year, new threats emerge faster than organizations can improve their defenses. Despite this perpetual challenge, security leaders continue to develop innovative strategies, adopt new tools, and assemble talented teams to combat information uncertainty. From the rise of cloud-computing to the evolving regulatory landscape, there are a myriad of issues to address.

Since 2014, Ari Kaplan Advisors has been engaging security leaders around the world in conversations about information management, insider threats, security investment, and an array of issues that impact an organization's defenses and data protection techniques. Ankura commissioned the analyst firm to speak directly to chief information security officers and senior corporate security leaders in order to determine how management has evolved, the patterns of concentration by corporate boards, and the cross-functional solutions being applied to address complex challenges.

SURVEY BACKGROUND

Ankura partnered with Ari Kaplan Advisors and interviewed 30 industry leaders in August 2017, to detect how corporations are adapting to today's evolving threat landscape. All spoke by telephone, under condition of anonymity, in August of 2017.

70% of the respondents serve as their organization's **chief information security officer**

3% serve as the **chief security officer**

3% serve as the **chief technology officer**

24% hold **vice president or director-level positions** with primary responsibility for information protection or cybersecurity.

70% were from **ORGANIZATIONS** with over **$1 billion** in annual revenue.

50% were from **COMPANIES with revenues** of more than **$5 billion**.

80% were from **COMPANIES** with over **5,000 employees**.

THEY HAILED FROM A DIVERSE GROUP OF INDUSTRIES, INCLUDING:

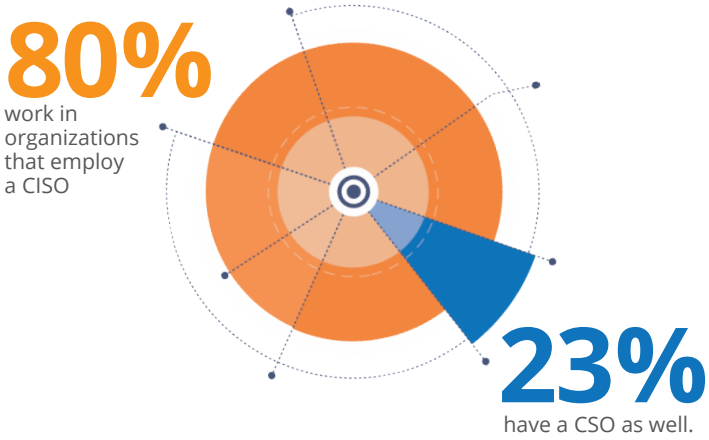
FINANCIAL SERVICES	30%	CONSULTING	3.3%
HEALTHCARE	16.7%	MANUFACTURING	3.3%
TECHNOLOGY	16.7%	MEDIA	3.3%
BANKING	10%	TELECOMMUNICATIONS	3.3%
INSURANCE	10%	RETAIL	3.3%

While most participants were based in the United States, the report does include perspectives from Europe and Australia. Given that 67% of the respondents were from the highly regulated financial- and healthcare-related industries, the responses skew towards strong levels of awareness about cybersecurity and data governance, whereas a review of the one-third from non-regulated industries reflects a more measured viewpoint.

EXECUTIVE SUMMARY

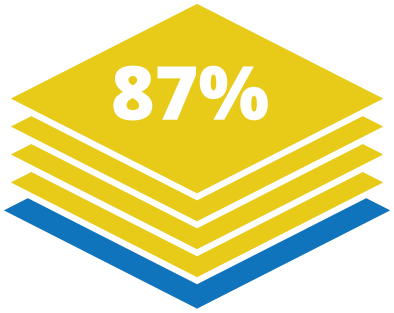
THE EVOLVING ROLE OF THE CISO

80% of respondents work in organizations that employ a CISO and 23% have a CSO as well. 53% of CISOs report to the chief information officer; 7% report directly to the chief executive officer; and the remaining participants report to their chief operating officer, chief risk officer, or another senior-level individual at the company. 57% report to senior management at least monthly, while 37% do so quarterly. 43% of participating CISOs report to their board of directors on a quarterly basis, while 20% do so monthly, 13% semi-annually, and 10% annually.



CISOs ARE CAUTIOUSLY ADAPTING TO THE CLOUD

87% of respondents reported that they rely on vendors or cloud-hosting providers to host non-critical information to save money and streamline their operations. Some are also trying to upgrade their infrastructure or responding to an enterprise-wide initiative to innovate. 17% of the respondents noted that Office 365 is a common impetus for moving to the cloud.



reported that they rely on vendors or cloud hosting providers to host non-critical information to save money and streamline their operations.

OUTSIDE SUPPORT IS ESSENTIAL

100% of respondents work with third parties to support their security initiatives, and 87% use third parties for ongoing project or program support. While 97% formally evaluate the security practices of their vendors, partners, law firms, and third parties that interact with their data, 60% of respondents do not extend this level of inquiry to the partners of their third parties.

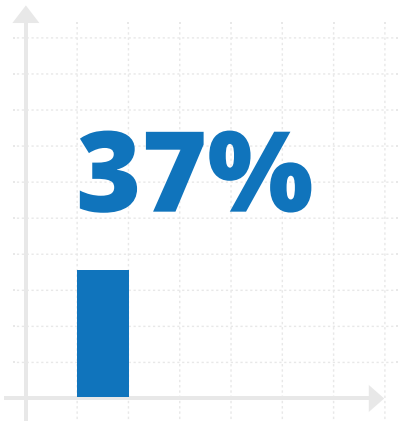
100% work with third parties to support their security initiatives

97% formally evaluate the security practices of their vendors, partners, law firms, and third parties that interact with their data

60% do not extend this level of inquiry to the partners of their third parties.

MANAGED SERVICES PROVIDERS TYPICALLY SUPPORT CYBERSECURITY

77% of respondents advised that the scope of their managed security services includes incident response. And, for 63%, that support included onsite response. 37% were confident that their managed services provider would provide a legally defensible investigation if they were the victim of a breach or other cyber incident. 30% claimed to be very confident.



37%

were confident that their managed services provider would provide a legally defensible investigation if they were the victim of a breach or other cyber incident.

SECURITY AND BYOD POLICIES ABOUND

100% of respondents reported having data security and incident response plans. All of the respondents noted that they have a privacy policy or program, but 13% described it as "insufficient or incomplete." 87% reported that their organizations have both a disaster recovery plan and a data governance framework or committee in place. 80% reported having a Bring Your Own Device (BYOD) plan, though some noted that their plan is to prohibit personal devices. 63% believe that those gadgets contain company sensitive information.

100%

OF RESPONDENTS

reported having data privacy and incident response plans.

13%

DESCRIBED THEIR

privacy policy or program as "insufficient or incomplete."

80%

REPORTED HAVING

a Bring Your Own Device (BYOD) plan.

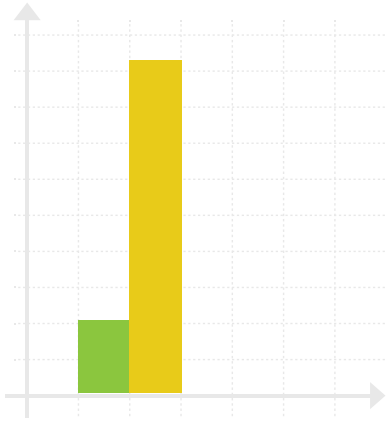
63%

BELIEVE THAT

BYOD plan gadgets contain company-sensitive information.

SECURITY MESSAGING IS EVOLVING WITH TRAINING AND COMMUNICATION TRENDS

While 93% reported focusing their messaging on employees: being part of the solution, 20% still claimed to leverage fear to grab the attention of their employees. Despite the 20% who choose fear, a number of security leaders provided reasons for avoiding it. 20% also noted offering best practices to avoid risk.



93%

reported focusing their messaging on employees being part of the solution

20%

still claimed to leverage fear to grab the attention of their employees.

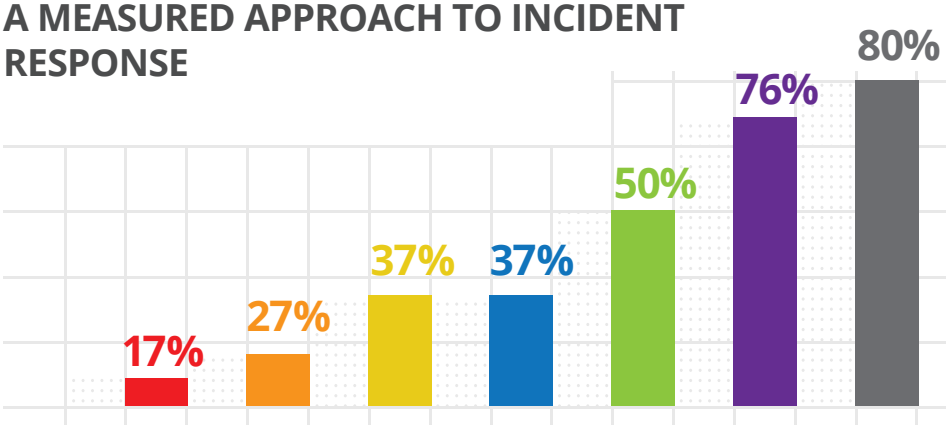
SUCCESS OF SECURITY INVESTMENTS IS MEASURED BY RISK REDUCTION.

93%
of respondents focus on risk reduction as measure of return on IT security investments.

70%
are interested in improved detection capabilities.

20%
characterized the amount they had spent on IT security in the past two years as insufficient.

BALANCED BREACH POSTURE REFLECTS A MEASURED APPROACH TO INCIDENT RESPONSE



- worried most about ransomware or malware
- focused on cyber attacks
- concerned most about an employee mistake
- characterized their information security it as proactive
- described their information security posture as equally reactive and proactive
- ranked user threats as their greatest area of weakness for enterprise security visibility
- concerned somewhat or very concerned that they had already been breached

50% of the respondents described their information security posture as equally reactive and proactive, with an additional 37% characterizing it as proactive. 80% of the respondents were somewhat concerned or very concerned that they had already been breached, and 37% were most concerned about an employee mistake, followed by 27% focused on cyberattacks, and 17% most worried about ransomware or malware. And, 76% ranked user threats as their greatest area of weakness for enterprise security visibility.

DATA MANAGEMENT IS A MYSTERY FOR SOME

77% of respondents claimed to have a data map of their organization's information landscape.

30% described their organization's data management as "ineffective or out of date."

97% can identify critical-value data within their networks.

60% have a way to know what people do with the critical-value data after it is accessed.

83% have the means to identify who accesses critical-value data.

KEY FINDINGS

THE EVOLVING ROLE OF THE CISO

As concern over cybersecurity has increased, so has the growing influence of the chief information security officer. In fact, 80% of respondents work in organizations that employ a CISO, and 23% have a Chief Security Officer (CSO) as well. 53% of CISOs report to the CIO, 7% report directly to the chief executive officer, and the remaining participants report to their chief operating officer, chief risk officer, or another senior-level individual at the company. 57% report to senior management at least monthly, while 37% do so quarterly.

THE CISO AND THE BOARD OF DIRECTORS

43% of participating CISOs report to their board of directors on a quarterly basis, while 20% do so monthly, 13% semi-annually, and 10% annually. Despite the fact that 63% of respondents report to their board at least monthly, there are challenges generally related to setting expectations, improving the impression and understanding of security, and emphasizing the importance of security to board members for purposes of allocating appropriate funding.

When the board is involved and there is support for security initiatives at the highest level, results improve, though it may take time and remain a work in progress. "There were some misunderstandings four years ago, but none today," reported the chief security officer for a large healthcare company. Even with support, however, there may still be philosophical variations. "We are lucky that the president and senior staff are very familiar with cybersecurity issues, but I think the president thinks that security is a lot like operations, which is not the case," added a director of information security for a bank. "The understanding of how security operations function and can weigh on the company is deficient," the director added.

One respondent recommended that companies encourage security executives to join boards to help drive the maturity of security programs. This initiative increases security awareness through discussions at the board level and highlights where it plays a role in the organization.

RESETTING EXPECTATIONS

As data protection becomes more complex and the threat of loss or theft becomes increasingly sophisticated, security leaders must continue to adjust the conversation with management. "It is more about expectations of what it takes from a personnel perspective, because security is an insurance policy that no one wants to pay for," advised the senior director of information security for a telecommunications company.

Decision-makers require continuous validation that security investments are good for business and thus must be informed about threats and vulnerabilities. "They think we are not being attacked and we have to continue to show metrics that indicate internal attacks to support our efforts and budgets; the struggle is not in keeping up, it is in keeping ahead," noted the CISO of a healthcare company.

The obstacle is not only to show that attacks are ongoing, but also that they can come from any direction. "Most people outside of the security profession view the threat as external; it is not the nation-state hacker from Russia that is hacking us as much as it is an insider doing something stupid," added the CISO of a financial services firm.

ENCOURAGING UNDERSTANDING

While cybersecurity has become a much more common term, which regularly appears in the mainstream news, there is still confusion about the definition of cybersecurity. "Cyber indicates that you use technology, but information assurance goes beyond technology," said another financial services CISO. "Our response and recovery capabilities have nothing to do with technology; too many people think that security is a technology problem, which is incorrect," the individual added.

For that reason, it is essential for security leaders to educate members of the board and fuel an appreciation for the array of issues included with a cybersecurity campaign. "It is so technical that boiling it down into chunks for the board to understand is the biggest struggle," remarked a CISO in healthcare. "It takes a lot of education of technical details and building trust; it is also critical to have advocates on the board, as that is a big win."

The investment involved and the selection of adequate solutions to address the problem are key concerns. "The biggest misunderstanding is that a company can throw a bunch of money and the problem is solved; it is an ongoing business problem and is an annual cost of doing business," advised a CISO in financial services. "Many who understand technology still think of it as it was 20 years ago; they think you can catch everything and that a firewall is sufficient," added another in the insurance industry.

Strong security strategies are cross-functional and incorporate the entire organization.

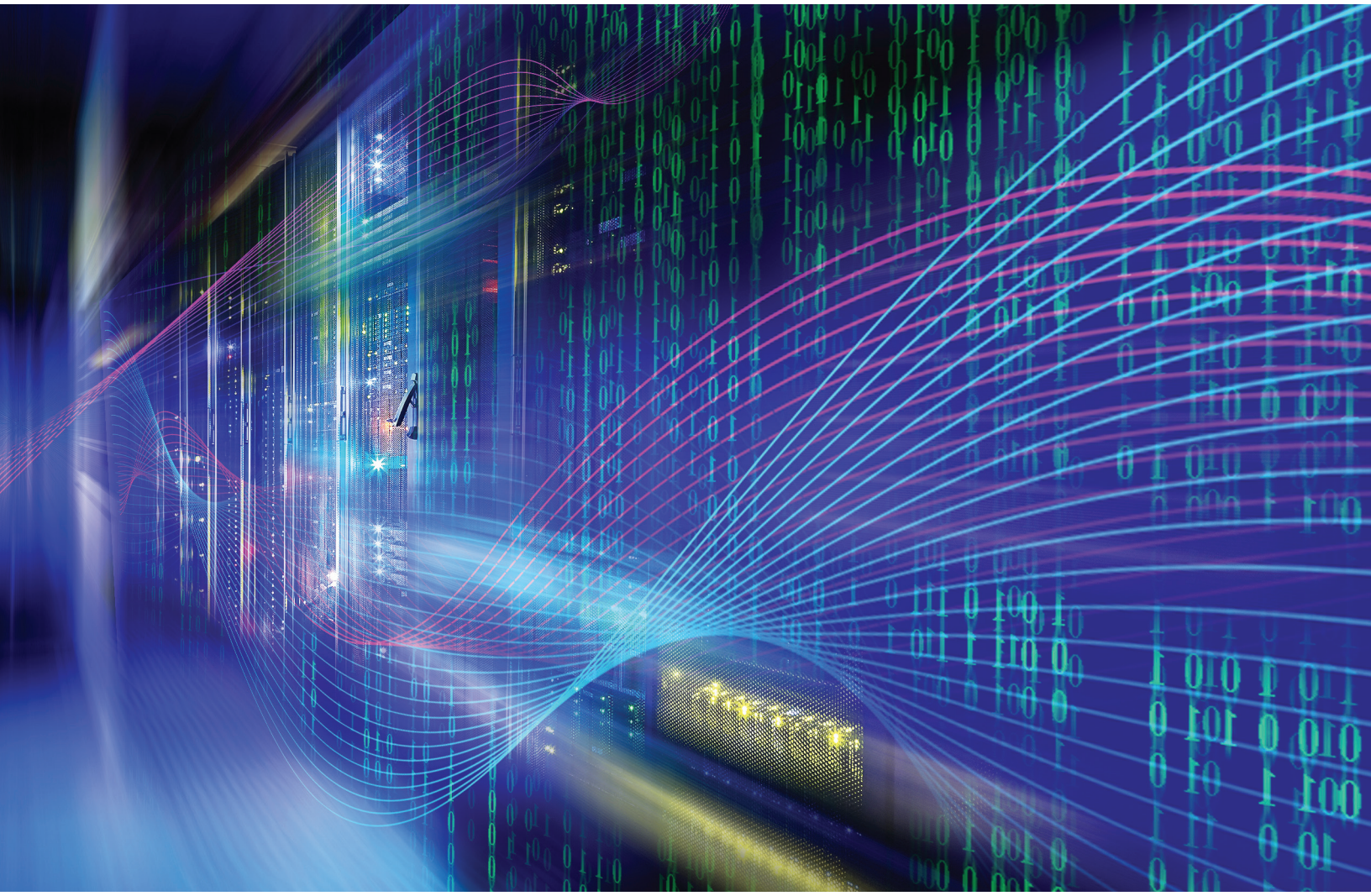
INFLUENCING THE IMPACT

Routinely discussing and setting expectations, and encouraging greater understanding of the security landscape helps organizations align the risk and impact of any potential event. "It is an issue of senior management or board members understanding what the risk actually means in terms of financial exposure," said the CISO for a bank. "The challenge of the CISO is to explain the technology issues and relate them to the business."

The hurdle is that while those who populate the board tend to have industry-specific knowledge, business acumen, and domain experience, "they are not technical people, so they generally don't understand the nature of the risk, the existing systems, and the impact of those systems being compromised," noted the head of physical security for a technology company.

Even if they do recognize the impact, there is an issue of sustainability. "They react to what is in the media or concerns that are brought to their attention, but they forget quickly; they don't realize that in order to maintain a certain level of assurance, it requires a sustained commitment," added the IT director for a healthcare company.

The director of information governance for a financial services firm summarized the unease over data management. "They don't understand the relationship between security and everything else around it," the individual noted. "If you get rid of data correctly, you don't have to worry about security, but they are effectively deprioritizing security by ignoring peripheral domains like records management, privacy, and discovery." As a result, it is essential for senior executives and board members to appreciate the relationship between privacy, cybersecurity, and the data life cycle.



CISOs ARE CAUTIOUSLY ADAPTING TO THE CLOUD

87% of the respondents reported that they rely on vendors or cloud-based providers to host their data. Most of them are trying to move non-critical information to the cloud to save money and reduce the location options for their records. They are also trying to upgrade their infrastructure and retire obsolete technology, but the information security department is not always encouraging this shift. "The security team is receiving pressure from IT operations, which is driven by value, cost-savings, and manpower-reductions," commented the director of information security for a bank. "One of the core initiatives of the company is to embrace cloud technology and everything it has to provide," added a participating CISO who is implementing an enterprise-wide mandate.

Office 365, for example, is often a common impetus to moving to the cloud. "Office 365 is a big driver for the migration," said one participant, who echoed comments from 17% of the respondents. "30% of our data is hosted; that will ramp up because the company is migrating to Office 365," noted another.

Despite the support for the cloud, only one participant worked with a company that hosts all of its data externally. 80% of those who rely on external vendors or cloud hosting providers permit only "some" of their data to be hosted externally versus maintained on the premises to balance the risk. "The company uses a combination of cloud and internal solutions," said one vice president in risk management for a financial services firm.

"The company is a large consumer of Amazon Web Services (AWS), but also has one of the largest data centers that host customer data," added the CISO of a media company, who added: "I do not trust outside cloud-hosting providers due to our compliance and regulatory requirements, and the company has a highly developed innovation program where they develop products, so the associated data is highly encrypted."

Others were similarly cautious. "It is a hybrid approach, where the company has moved to a cloud environment, but keeps its 'crown jewels' on premises," advised a technology industry CISO. "The company will stay in a hybrid solution because it cannot be totally dependent on the cloud; if you are not a Fortune 500 company, you will not get the necessary attention," added a CISO who also serves as the financial services firm's chief technology officer. This composite approach is often successful only when organizations streamline their data management, given that almost one-third of the participants described their data maps as "ineffective or out of date" (which this report addresses in detail).

Still, 70% are planning to migrate data or systems to the cloud in the coming year. "It is currently less than 10%, but if you ask me that question next year, it will be 50%," said a CISO in the same industry. "The company empowers employees to work everywhere [so] the mandate is cloud first," a CISO based in Australia remarked.

One fundamental reason for the mistrust of the cloud is the inability to truly verify its operations. "The biggest impediment to use of the cloud today is that people don't understand security in the cloud," said one CISO in financial services. Also, "once you get past the contract and they sign the indemnification clause, it is a crap shoot," added another in healthcare. "If your vendor is feeding you a bunch of lies and doesn't have the processes that they are supposed to under law, you can try to detect them, but you really don't know." One director of information security for a bank advised that you can gauge the service provider's strength in this area by asking questions about its vendor management programs and contractual obligations. "There are 90 to 100 questions just on the vendor management of our partners and third parties," the individual advised. "In addition, the company requires validation of those responses in the form of back-up documentation; it is not just an ask, it is an ask and validate."

Although organizations and business leaders are convinced that relocation to the cloud is inevitable and for the best, security professionals are sensitive to the increased risks, greater exposure, and uncertainty associated with the rights and responsibilities of the cloud provider.

OUTSIDE SUPPORT IS ESSENTIAL

100% of respondents work with third parties to support their security initiatives. "Certain aspects of the business use them for ongoing support," said one media company CISO. Another in financial services highlighted that his company uses an external provider for "level-one security monitoring." With the increased emphasis on remaining at least one step ahead of potential threats, consistency in this effort is critical, which is why 87% use third parties for ongoing project or program support.

Given that every company surveyed works with third parties, it was not surprising that 97% formally evaluate the security practices of their vendors, partners, law firms, and third parties that interact with their data. For 17% of them, regulatory requirements have driven that effort. "This is a huge initiative since it is a requirement of regulators for all financial services companies and the General Data Protection Regulation (GDPR); the company calls this vendor management risk." The GDPR will influence the way many companies appraise their partners, given the expansion of responsibilities for both data controllers and processors under the new privacy framework set for implementation in 2018."

Despite its importance, 60% of respondents do not extend their due diligence to the partners of their third parties. Many rely on formal agreements for protection. "They are contractually obligated to hold their contractors to the same set of standards that we require of them," said the chief technology officer for an online retailer that does not proactively inspect these "fourth parties." "The company looks only at its own third parties, but asks for verification that those entities have looked at their own third-party protocols; it is a liability transfer effort," added a peer.

The challenge associated with transferring liability is that while an organization may secure a legal victory, it could ultimately be a Pyrrhic one since the public typically recalls only the high-profile brand name of the breached company, rather than the name of the vendor actually breached or whose technology failed. And, when that failure occurs, the job at risk is rarely that of the third party's project manager or systems administrator. Instead, there are often public resignations of C-level executives who are forced to take responsibility for an issue for which they may have no direct culpability.

Despite that uncertainty, a majority of respondents (53%) suggested that they were confident in the security of their data managed by vendors, partners, and third parties. One-third, however, were either unsure or not confident. Only 13% claimed to be very confident. "I can't get to 'very confident' yet until we start doing fourth-party reviews; many third parties have a third party managing their data, [so] until until you get to fourth- and fifth-party reviews, you cannot be very confident or shouldn't be," said the CISO for a major bank.

These factors are critical because 57% of the participants noted that their organizations are periodically involved in litigation or investigations that require them to transfer information to law firms and eDiscovery vendors, among others. 27% frequently need to do so. "It depends on the case and litigation, as well as what disclosure of information is required," commented a technology CISO.

That said, while all data management vendors at one health care company must undergo a formal risk assessment, "Regarding law firms, since they have evidence data and not necessarily electronic protected health information or personally identifiable information, the company typically does not evaluate their security practices except in a few evidence data sets where PII is embedded," said one CISO. "Not comfortable at all for law firms," cautioned another in financial services.

MANAGED SERVICE PROVIDERS OFTEN INCLUDE INCIDENT RESPONSE SERVICES

77% of respondents advised that the scope of their managed security services includes incident response. And, for 63%, that support includes on-site response, if necessary, but the opinions on this issue were mixed. "Typically, managed security services providers are responsible for outsourced security review, but the company handles incident response in-house," advised the CISO for a technology company. "I don't believe in outsourcing incident response; I always like to control my own incident response because it is just too central to everything," added another CISO in the same sector.

That said, 37% are confident that their managed services vendor will ensure a legally defensible investigation if they are the victim of a breach or other cyber incident. 30% claimed to be very confident. "There is no such thing as being very confident in security," said one CISO; yet, thosewho were very confident had worked with their managed services provider for some time and trusted its experience. Also, many respondents were confident in the limited responsibilities they assigned to their external support teams. "We are not looking for managed services to run the incident, just looking for them to drive awareness and facilitate calls that involve the handoff to the internal group," said the director of information security for a manufacturing company.

SECURITY POLICIES AND BYOD

100% of respondents reported having data security and incident response plans. All of the respondents noted that they have a privacy policy or program, but 13% described it as "insufficient or incomplete." 87% reported that their organizations have both a disaster recovery plan and a data governance framework or committee in place, but one head of physical security described the latter as "more concept than practical so there is a lot of discussion about it, but it doesn't get a lot of attention."

80% reported having a Bring Your Own Device (BYOD) plan, though some noted that their plan is to prohibit personal devices. 63% believe that those devices contain company-sensitive information. "I'm sure somebody snuck something on there somewhere," said a healthcare CISO, but most comments focused on the protective nature of their protocols. "The company has various controls in place to prevent this," said one security leader, who echoed comments by others that device data is "sandboxed" for protection. "It is in a containerized environment for protection," added another CISO.

SECURITY MESSAGING IS EVOLVING WITH TRAINING AND COMMUNICATION TRENDS

While 93% of respondents focus their messaging on employees being part of the solution, 20% still leverage fear to grab their attention. "Fear seems to work pretty well because it gets their attention, but being part of the solution is also effective because it gives a shared sense of ownership of the company's fate," reported a director of information security in telecommunications.

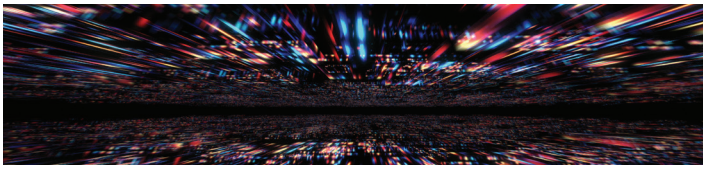
Despite the 20% who choose fear, a number of security leaders provided reasons for avoiding it. "People aren't stupid; fear only gets you so far," said a banking CISO. "Empathy and understanding their problems is the best way to get them to participate and in finding an equitable solution," the individual added. Fear doesn't do jack; people may get scared, but they will not do anything meaningful [to prevent incidents]," remarked another CISO in financial services.

20% also offer best practices to avoid risk. "When someone sends a message alerting [information security] about a potentially damaging e-mail, they are acknowledged and praised to their management," reported a director of information security. Ultimately, though, "anytime you can get end users involved in the process to understand security and feel that they are part of the process, you get better results than [if you are simply] forcing something down their throats."

Almost every participant discussed offering periodic user awareness training, email alerts, and targeted marketing. "It is literally in everyone's face every single day, including on the front page of the company's intranet," said a vice president of risk.

Some offer regular security tips, banner ads on the company's intranet, phishing prevention tests, internal social networks, town hall meetings, and games. Some also collaborate with other groups within their organization to reinforce the expectations. "The company works with the compliance team and adapts to its messaging," noted a healthcare CISO.

SUCCESS OF SECURITY INVESTMENTS IS MEASURED BY RISK REDUCTION



93% of respondents focus on risk reduction as a measure of the return on their IT security investments, followed by 70% interested in improved detection capabilities. "Risk reduction is paramount," said one CISO. "We use efficiency of incident response, frequency of incident identification, and improved detection capabilities in our overall evaluations, but not to measure the return."

While 57% characterized the amount they had spent on IT security in the past two years as sufficient, 20% advised that it has been insufficient. There are a variety of factors that have helped the respondents make this determination. Some have already made significant investments so their existing spending is sufficient to maintain their portfolio. Others are perpetually paranoid and always feel unprepared. "I have to be faster than the bad guy, so I always have to assume that I'm behind the clock," said a director of information security.

One participant explained, "The issue is tying the expense to a risk that is sufficient to get those who manage the budget excited [enough] to address it, rather than devote those resources to research and development." Another noted, "That is a subjective question based on our IT budget, our revenue, our size; I have been given as much as I've asked for, but I have never met a CISO who would say that their spending is high."

Despite concerns about budgeting and investment returns, 30% of the respondents allocate 4 to 7 percent of their overall IT spending to information security. That said, however, one-third of those individuals characterized the amount they have spent on IT security in the past two years as "insufficient." 17% allocate more than 13% of their budgets to information security.

For 73% of respondents, regulators are driving budgeting decisions. That is followed by 53% who name the value of their data as a major budgetary driver.

BALANCED BREACH POSTURE REFLECTS A MEASURED APPROACH TO INCIDENT RESPONSE

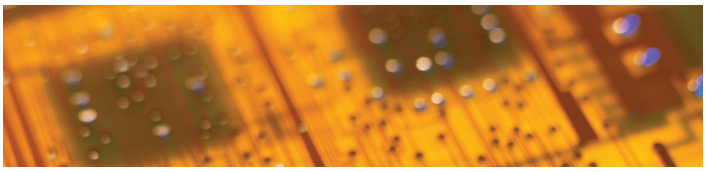
50% of the respondents described their information security posture as equally reactive and proactive, with an additional 37% characterizing it as proactive. 80% of the respondents were somewhat concerned or very concerned that they had already been breached, and 37% were most concerned about an employee mistake, followed by 27% focused on cyberattacks, and 17% most worried about ransomware or malware. And, 76% ranked user threats as their greatest area of weakness for enterprise security visibility.

57% were most concerned about the theft of personally identifiable information.

80% ranked their own ability to detect and respond to a data breach at a seven of higher out of 10. As part of that effort, most organizations had employed both an incident simulation (87%) and a tabletop exercise (93%) in the past year. In fact, 83% found the tabletop exercise to be effective in promoting strong cybersecurity hygiene throughout their organizations because it raised awareness and enhanced preparation.

Further, 93% have established a multidisciplinary incident response team, and 47% were most concerned about their ability to accurately diagnose what data may have been exposed, followed by 27% who were anxious about identifying an incident.

DATA MANAGEMENT IS A MYSTERY FOR SOME



Although 77% of respondents claimed to have a data map of their organization's information landscape, 30% described it as "ineffective or out of date." "Most of it is intuitive; it is not a formalized document," remarked one security leader.

While 97% could identify critical-value data within their networks, and 83% have the means to identify who within their organization accesses that critical-value data, only 60% have a way to know what people do with the critical-value data after they have accessed it. "I know if they download it or move it, but if they are viewing it from outside of the system, I cannot completely tell," admitted one CISO. "We are more focused on making sure that it is not "exfiltrated" and less concerned about what they do with it within the company's network," highlighted another security leader.

To strengthen their security posture, 77% of respondents assign ownership of data or systems to individuals within the company. Department heads or business unit leaders are typically the data stewards. Still, there is tremendous uncertainty. "No one knows where their data is, who owns it, what's out there, why it is out there, and who is accessing it; it is the big unknown," remarked a CISO in technology. "We really need to understand the data, where it is, and how to classify it to properly protect it; many security programs are backing into that now because it doesn't exist, but it is difficult when you don't know all of the facts about your data," added the director of information security for a telecommunications company.

LOOKING FORWARD

MORE FINANCIAL SERVICES COMPANIES WILL HIRE CISOs OR ENGAGE VIRTUAL CISOs

The participants reported that the median number of external providers who support them was 7 to 10. "We outsource most of the work that the internal technology team does not have time to do," said the CISO for a smaller financial services institution. For the 20% of respondents who do not have a CISO, the CTO, COO, or deputy security official assumes that role. 40% of those companies have revenue under $1 billion.

40% of the respondents noted that they are subject to 23 NYCRR 500, the state of New York's new Cybersecurity Requirements for Financial Services Companies, which mandates that a company designate a CISO, either internally or from an external resource. It is likely that the role of the CISO will continue to become more prominent. This is particularly important for smaller companies without a CISO that now need to either hire one on a full-time basis or engage a third party to provide those services.

DATA MAPPING IS LIKELY TO EXPAND

Although 77% of respondents work for organizations that maintain data maps, 30% of them described those documents as ineffective or out of date. As a result, it is likely that they will update existing records and more companies will develop them, given the challenges associated with the data landscape. "We would desperately love to do that and are making baby steps," reported a bank CISO. "It is the ultimate blind man feeling an elephant, as it describes a situation that is so big, but you have no idea how to get started," the individual added. A CISO with an insurance company highlighted that the regulatory environment is also driving the importance of this effort. "Encryption at rest is required by the New York regulations, and in order to do that, you need a data map."

CLARITY MAY CHARACTERIZE CYBER LIABILITY INSURANCE

While 83% of the participating CISOs advised their companies on the purchase of cyber liability insurance and 67% maintain such policies, there is a consistent call for clarity in these agreements. As the size, scope, and frequency of these claims rise, the documents may provide a more thorough outline of the coverage limitations going forward. "The cyber policies we've reviewed have so many waivers and limitations within them that if we had a breach, they would not cover us," said a healthcare CISO. "We have looked at them and have gone through the exercise of evaluating peers because when you assess the items that they exempt, we did not feel like we were getting our money's worth; we would rather be self-insured," added another in the insurance industry.

FOCUS ON NEW REGULATIONS, INCLUDING GDPR, SHOULD RISE

Since 73% of respondents noted that regulators are driving their IT security budgeting decisions (and that was 20% more than the next most significant factor, *i.e.*, the value of their data), and that 100% of the participants advised that there is at least one regulatory framework that applies to their business, the focus on an increasingly dynamic regulatory environment is likely to rise.

Most important, although 60% of those surveyed noted that GDPR is important to their organizations and 87% have a privacy policy or program, given the global interest in the new framework and its impending May 2018 enforcement date for non-compliance violations, organizations are likely to concentrate on its influence more closely in the coming months. "We are still assessing the impact of GDPR," said one financial services CISO. "GDPR, International Traffic in Arms Regulations (ITAR), and Export Administration Regulations (EAR) are somewhat important, but the company does not do business in Europe," added another for an insurance company. Despite their reservations, organizations that do not fully understand the impact of the GDPR (in that it could apply to companies that do not necessarily conduct direct transactions in Europe) or have not already started evaluating GDPR are unlikely to achieve the appropriate level of compliance.

INSIDER THREAT PROGRAMS AND POLICIES MAY INCREASE

While 63% of the respondents have an insider threat program or policy, this number is likely to increase, especially since an employee mistake was the security incident about which the largest number of respondents (37%) were concerned. One financial services CISO noted that "an insider threat could encompass an employee mistake, a cyberattack, or a malware attack."

For the 37% of security leaders whose organizations do not maintain an insider threat program or policy, the increased risk associated with data theft from those with authorized access may change their strategy. "We have never thought it was worthwhile; I see no value in it," said a CISO in healthcare. "We are not as focused on insider threats due to the nature of the company; there are not a lot of lower-level employees, so it is not as big an issue," added an insurance industry CISO.

In addition to the uncertainty associated with employee behavior, many organizations have weak data policies in general. "The data stuff is usually completely out of the control of the security team; most of the time, nobody has control of it, which is part of the problem," said a CISO in financial services. The combination of fragile information governance coupled with the prominence of insider threats increases the likelihood that more organizations will develop strategies to combat this potent combination.

CONCLUSION

Uncertainty in today's cybersecurity landscape is not slowing positive change in information management, emerging threat response, and global data protection efforts. Most organizations recognize the need for security influence in the C-suite, all have incident response plans, and almost everyone in this area recognizes the value of investing in infrastructure to promote risk reduction. By emphasizing training, communicating effectively and acknowledging the increased influence of the cloud, companies of all sizes in most industries are succeeding in greater numbers. This trend will continue if organizations prioritize informing leadership, applying a successful risk management strategy, and collaborating with strong cybersecurity partners.

CONTACT US

For more information please visit our Cybersecurity expertise page:

ankura.com/expertise/cybersecurity

Compromise Detection

Ankura provides the client with an advantage by providing an evaluation of the ecosystem to indentify security issues through the utilization of experienced, highly skilled incident responders.

READ MORE

Incident Response

Ankura professionals have the in-depth experience to remediate the issue and inform critical decision-making for stakeholders.

READ MORE

Cyber Investigations

We draw on our collective private sector and law enforcement expertise and conduct cyber investigations in a professional and legally defensible manner.

READ MORE

Response Preparedness

Ankura's cyber experts have deep experience in leading cyber incident response teams, plan develeopment, and forensic investigations, and assessing information security policies.

READ MORE

Data Governance and Compliance

Ankura has developed a unique, simplified and consolidated approach that empowers entities of all shapes and sizes to maintain a healthy data ecosystem and enebles better data oversight, compliance, utilization, and protection simultaneously.

READ MORE

Compliance Advisory and Assurance

We provide expert independent assessments of clients' compliance with, and audit readiness for, many of the most pervasive standards and regulations in key industries, as well as practical, no-nonsense roadmaps toward compliance validation and certification.

READ MORE

Crisis Preparedness & Operational Resilience

Being ready for and resilient to the possible, plausible, and probable.

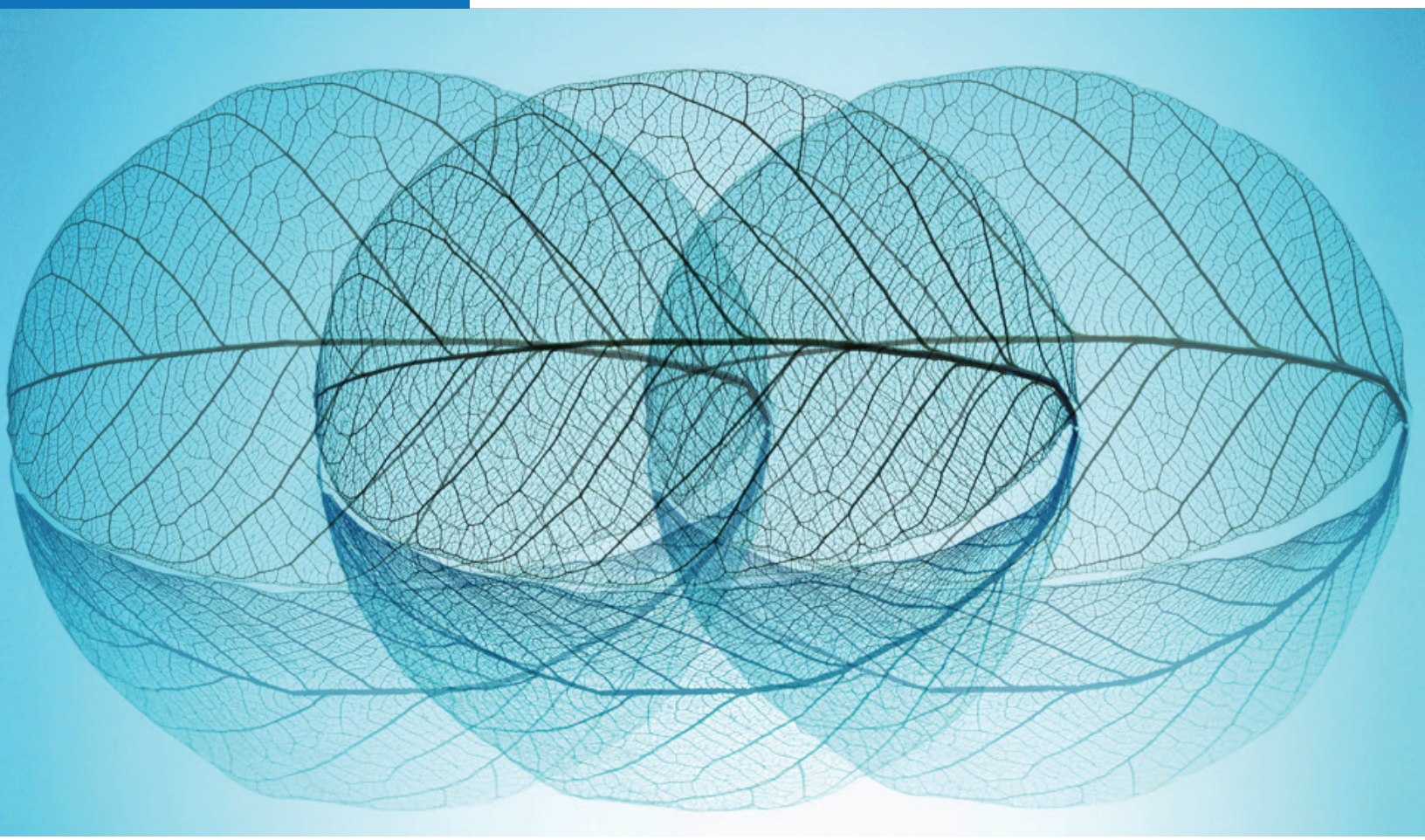
READ MORE

DATA BREACH RESPONSE

Ankura **cybersecurity experts** are available to provide **immediate assistance** if a breach is suspected.

PLEASE CONTACT US: ankuracyber@ankura.com or +1.844.540.0161

ABOUT US



ABOUT ARI KAPLAN ADVISORS

Ari Kaplan Advisors provides market research, ghostwriting, and benchmarking on trends associated with legal technology, cybersecurity, law department management, and law firm growth.

For more information please visit: **arikaplanadvisors.com**

ABOUT ANKURA

Ankura is an expert services firm defined by *HOW* we solve challenges. Whether a client is facing an immediate business challenge, trying to increase the value of their company or protect against future risks, Ankura designs, develops, and executes tailored solutions by assembling the right combination of expertise. We build on this experience with every case, client, and situation, collaborating to create innovative, customized solutions, and strategies designed for today's ever-changing business environment. This gives our clients unparalleled insight and experience across a wide range of economic, governance, and regulatory challenges. At Ankura, we know that **collaboration drives results**.

For more information please visit: **ankura.com**