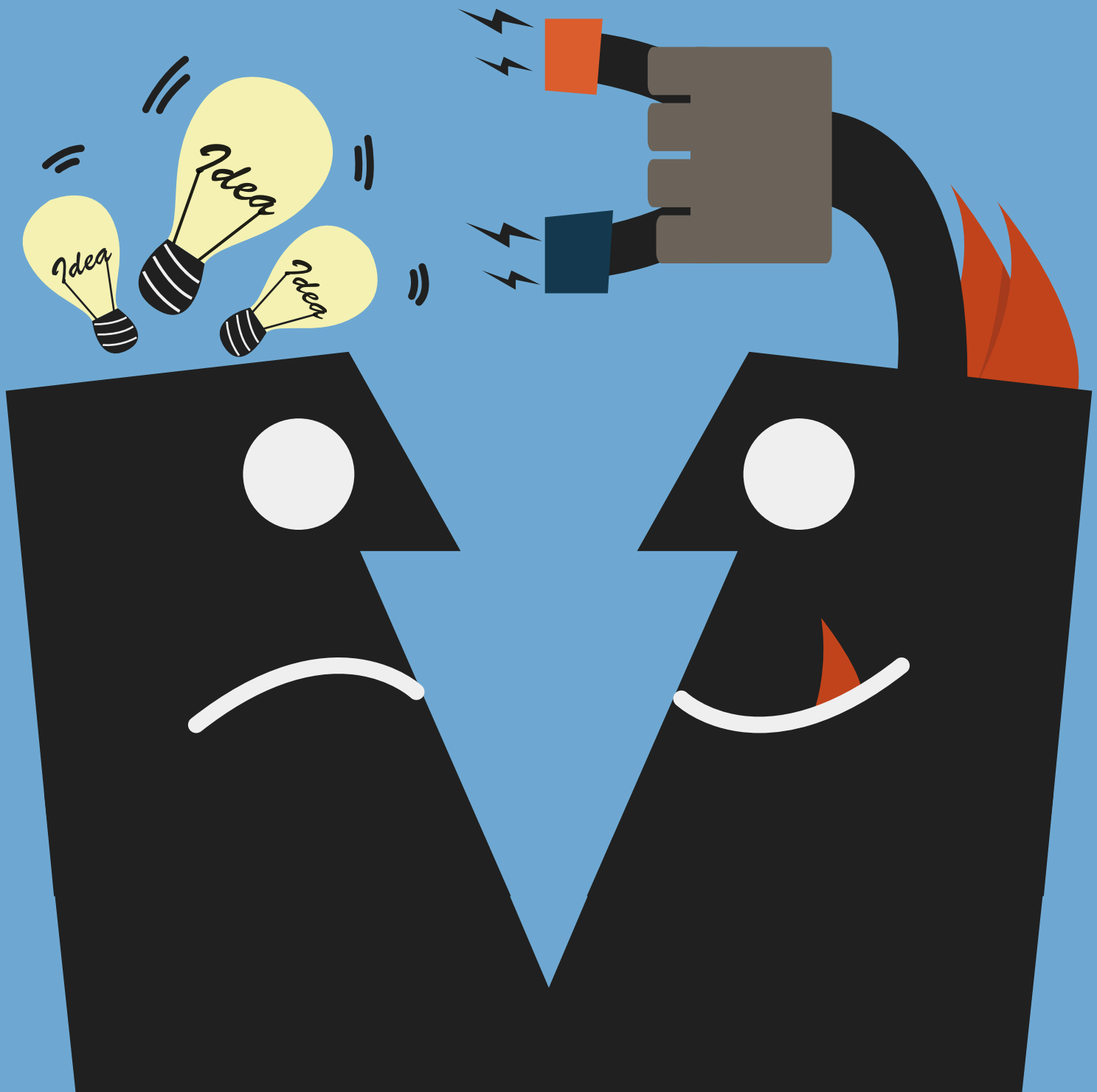
nuix

Simple. Powerful. Precise.

ARI KAPLAN ADVISORS

Defending Data:

Turning cybersecurity inside out
with corporate leadership perspectives on
reshaping our information protection practices



Defending Data:

Turning cybersecurity inside out
with corporate leadership perspectives on
reshaping our information protection practices

Contents

About Ari Kaplan

Ari Kaplan, a leading legal industry analyst, is an inaugural Fastcase 50 honoree and a finalist for ILTA's 2015 Thought Leader of the Year award. His most recent book, *Reinventing Professional Services: Building Your Business in the Digital Marketplace*, was released in Japanese, and Thomson Reuters is publishing the second edition of *The Opportunity Maker: Strategies for Inspiring Your Legal Career Through Creative Networking and Business Development* in 2016.

He is the principal researcher for a variety of widely distributed benchmarking reports and has been the keynote speaker for events in Australia, Canada, the United Kingdom and throughout the U.S. Kaplan is also the founder of the Lawcountability® business development platform, a finalist for ILTA's 2015 Innovative Solution Provider of the Year award and a two-time Ironman triathlon finisher.

Key findings

Information security has evolved from an obscure topic of conversation among techies to a centre-stage concern in the C-suite. Its influence is growing in every aspect of business. Budgets reflect greater weight on security; staffing and training show new distinctions; battling potential breaches is now a collaborative effort; and the cloud continues to create conversation. Nuix engaged Ari Kaplan Advisors to interview 28 corporate security officials to capture the key trends and we summarise our findings below.

» Budget granularity is growing

More security officials are familiar with the proportion of the security budget their organisation dedicates to managing and protecting the perimeter versus responding to and remediating incidents. This year, 61% knew the breakdown of their security spending, compared to 54% in 2014.

» Regulatory impact on spending has doubled

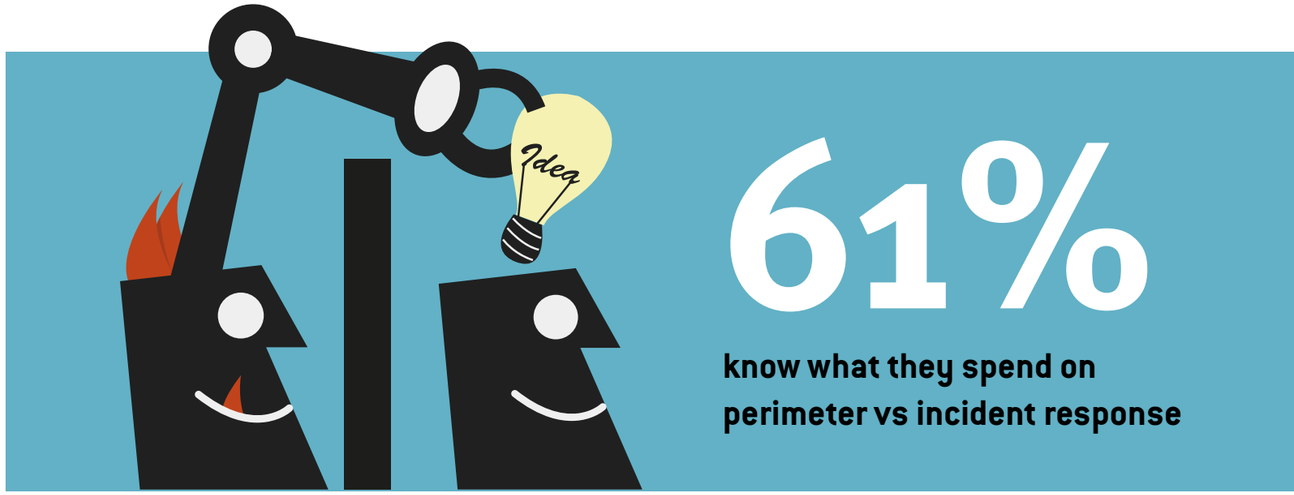
The shifting regulatory landscape is prompting organisations to modify their budgets to accommodate greater scrutiny. Half of the survey participants said regulators impacted their security spending, up from less than a quarter in 2014.

» A majority of respondents have insider threat programs

There is greater focus on insider threats. More than two-thirds (71%) of respondents reported having an insider threat program or policy; 21% attributed some of their security team's spending increases to additional protections against internal hazards and 14% reported allotting 40% or more of their budget to insider threats.

» Tracking insider activity is a challenge for some

Although almost all respondents (93%) reported being able to identify their critical value data, only 69% said they knew what people did with the critical value data after they accessed it.



61%

know what they spend on perimeter vs incident response

» Incident response readiness is in focus

Nearly all respondents (96%) said they had an incident response readiness policy and 68% claimed to test their responsiveness to ensure compliance with current policies and practices multiple times per year – 21% said they tested twice a year and 32% did so at least quarterly. More than one-third (36%) engaged in tabletop exercises and 46% provided actual responses to simulated threats.

» Byod on the rise

A large majority (82%) of respondents said their organisations had a bring-your-own-device (BYOD) policy – a material increase from the 69% of respondents who had one in 2014. The number of organisations that permit remote access is high but falling: 86% this year down from 96% in 2014.

» Human behaviour still an obstacle to security

An increased number of respondents claimed human behaviour was the biggest threat to their organisations' security – 93% this year, up from 88% in 2014. As a result, 39% chose fear, rather than best practices, as the most effective security messaging strategy to avoid risk, up from the 31% who selected that option in 2014.

» There is some consistency in cloud usage

The number of organisations migrating data to the cloud this year was down slightly to 71% from 73% in 2014, but the number migrating systems to the cloud dropped from 58% to 43%. This decline may be because many organisations have already moved their data and applications to cloud services. Again, a large majority of respondents agreed that use of the cloud created unique cybersecurity concerns (86% in 2015 vs. 84% in 2014).

» Executives are redefining the data breach

A quarter of the leaders surveyed were not concerned whether their organisations had been breached, while 32% described themselves as 'very concerned' about whether they had been.

To address security issues, 96% of executives said they shared and collaborated with other information security executives, an increase of four percentage points over 2014. A quarter of respondents said they interacted with colleagues in eDiscovery, legal, records management and information governance daily; all of them said they interacted at least monthly.

Cybersecurity: just a part of everyday business?

Cybersecurity has moved from being arbitrary and scary to an almost standard foe in the art of modern business. Now that most organisations have accepted the axiom that some level of data vulnerability is universal, many are graduating to an era of understanding, preparation and responsiveness.

How they execute on these variables has become a distinguishing feature between those who are ready for the inevitable and those who are destined to be front-page news. Organisations can take a wide variety of steps – encompassing policies, education, leadership, and technology – to combat a threat that has captivated the professional and commercial communities alike.

In 2014, the inaugural *Defending Data* report highlighted interesting trends associated with managing and protecting an increasingly ephemeral perimeter; a shift in security policies and procedures; and the evolving role of security officers. This year, there is more recognition of damage from insider threats; a lack of familiarity with an organisation's entire data landscape; and a rising appreciation for security among corporate executives.

Survey background

To track these and other developments influencing corporate security strategy, Nuix engaged Ari Kaplan Advisors for the second consecutive year to interview 28 corporate security officials with varying degrees of responsibility. All spoke by telephone, under condition of anonymity, between August and October of 2015.

Among the respondents, 21% served as their organisation's chief security or chief information security officer, while 61% were directors or vice presidents with primary responsibility for information or cybersecurity. The remaining 18% had management oversight for those areas.

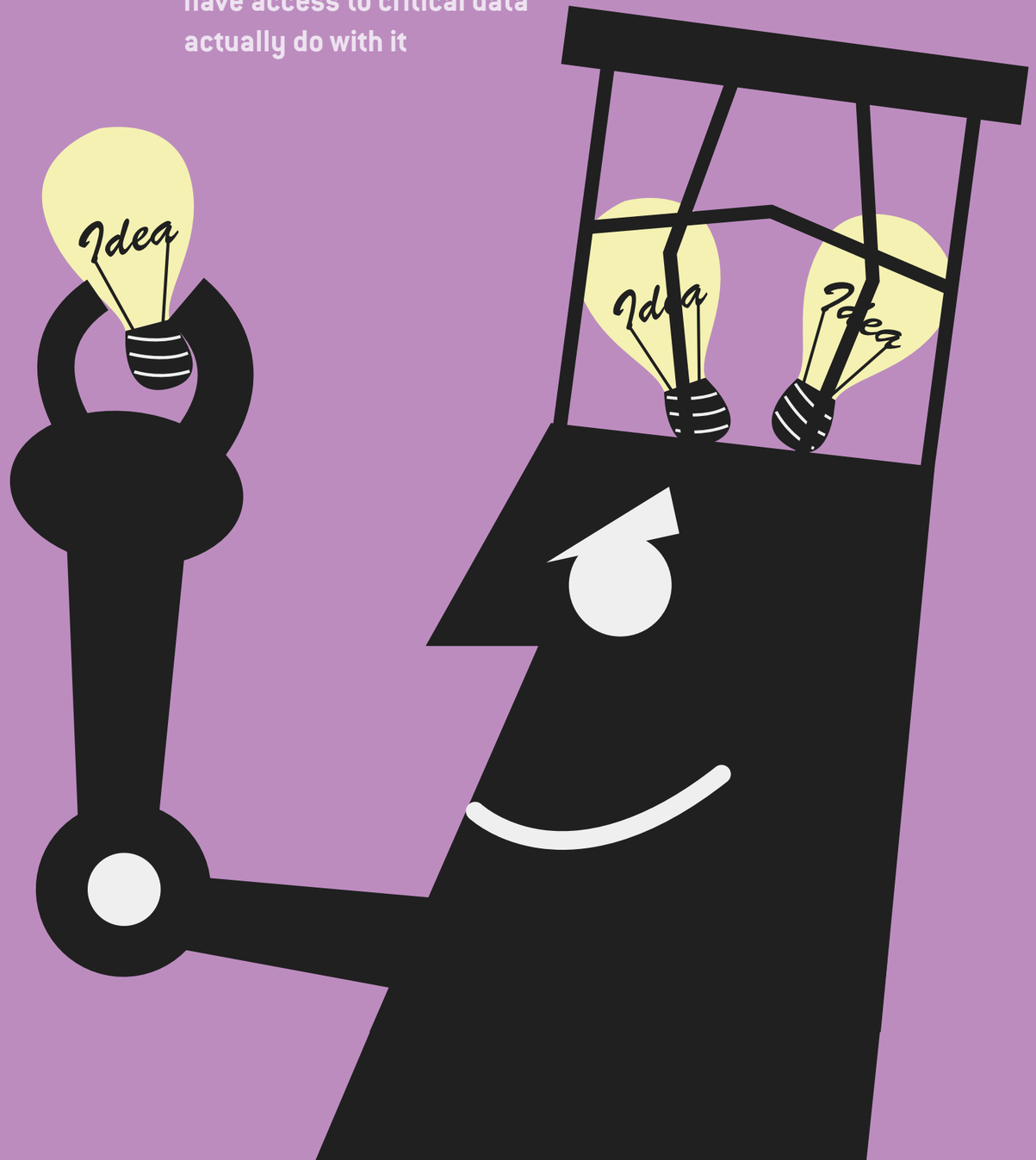
Three-quarters of respondents were from organisations with over US$1 billion in annual revenue and 57% with revenues in excess of US$5 billion. Most (71%) were from organisations with over 5,000 employees. They hailed from diverse industries, including:

- Financial services (32%)
- Life sciences (18%)
- Energy (11%)
- Banking (7%)
- Insurance (7%)
- Manufacturing (7%)
- Information technology (7%)
- Consulting (4%)
- Hospitality (4%)
- Entertainment (4%).

The respondents were about evenly split between highly regulated industries and more traditional sectors, which provided a balanced set of perspectives on the state of data security. Ari Kaplan Advisors also interviewed Keith Lowry, Senior Vice President for Business Threat Intelligence and Analysis at Nuix and Dr. Jim Kent, the company's Global Head of Security and Intelligence and CEO, North America.

31%

do not know what people who have access to critical data actually do with it



More clarity on budgets

In 2014, 46% of respondents did not know what proportion of the security budget their organisation dedicated to managing and protecting the perimeter compared to its spending on incident response and remediation. This year that number dropped to 39% reflecting an increased familiarity with capital outlay.

While there was a lack of consensus in 2014, 43% of those capable of providing estimates advised spending 50% or more on protecting the perimeter; 32% allocated 60% or more. About a fifth of respondents earmarked 80% or more to perimeter protection.

In 2014, 72% advised that spending in this area had changed in the past year and 65% expected it to increase in the future. This year, 89% claimed to have seen a change and 64% expected further increases.

Regulators continue to drive spending

In 2014, 23% of respondents highlighted that regulators impacted their spending posture; that number jumped to 50% in 2015.

“The regulatory landscape is constantly changing and that plays a huge factor,” said a financial services executive.

There is also a fear component, according to another in the same field: “For financial institutions, there are regulatory obligations, but you also have a duty of care and reputational risk; no one wants to be the CISO when it all goes horribly wrong.”

Additional drivers of IT security budgeting decisions included the nature of the data their organisations held, for 18% of respondents, and past experience for 11%. Another 11% noted that regulatory officials, data and transaction history all had a virtually equivalent impact.

Shift and increase in security spending related to rise of insider threats

In addition to increased regulatory oversight, 21% of the respondents attributed some of their spending increases to additional protections against internal hazards.

“Managing incident response and insider threats has received greater investment in the past year,” said one official with a global technology corporation.

“The company is not decreasing the amount spent on external threats, but it is increasing its spending on managing internal threats,” added a security leader with a life sciences organisation.

This year, 14% of survey participants reported allotting 40% or more of their budget to insider threats.

“There has been a shift in allocation toward looking internally, rather than at the perimeter,” said one security leader in the insurance industry. “The company is looking at data loss prevention technology to fight insider threats.”

Lowry attributed this renewed focus on three factors making insider threats more prevalent and worthy of protection:

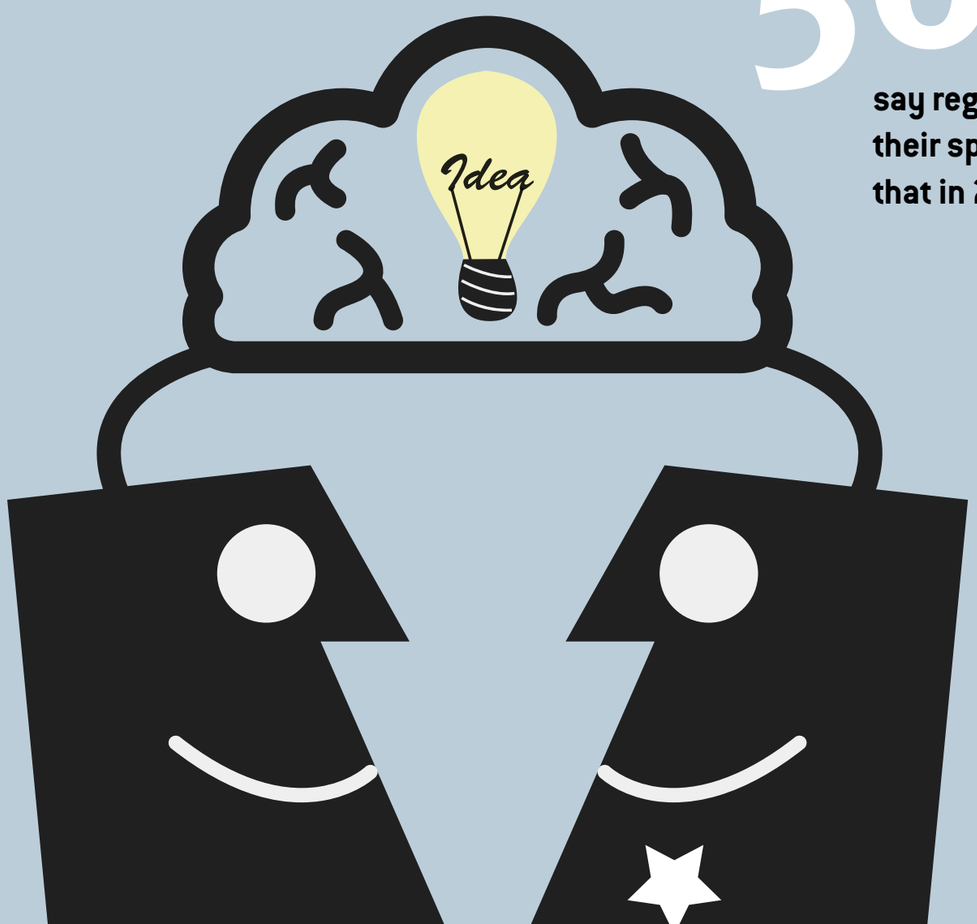
- Greater awareness of insider threats as a result of the public profiles of Chelsea Manning and Edward Snowden
- Widespread use of technologies that make it easier to steal information, e.g., you can copy vital files onto a USB thumb drive in seconds
- Theft of internal records has become culturally more acceptable.

On the last point, Lowry cited a survey conducted by technology business research firm Loudhouse, which found that 35% of decision makers and employees polled would willingly sell sensitive corporate information (or customer data stored on protected company servers) for ‘the right price.’ For 25% of the employees surveyed, that price was about $8,000 and for 18%, it was as little as $1,550.

“If you don’t take any action to an impending crisis, then someone will force you to take action,” Lowry advised.

50%

say regulators impact their spending, double that in 2014



Insider threat programs on the rise

Given this shift, it was not surprising that 71% of respondents reported having an insider threat program or policy. Of those, 90% had designated a senior official to provide oversight and 70% offered employee training in this area.

“The company employs intelligence teams that study different aspects of communications, user activity, social media, suspicious activity and other details,” said one bank director.

“We just received the authority to reinvent the company’s insider threat program; what was a program on paper only is now being funded and propelled forward companywide,” added an insurance executive.

Definitions of ‘insider threat’ vary

When asked to define the term ‘inside threat,’ there was a clear theme among the responses, featuring the words ‘malicious,’ ‘internal,’ ‘authorised,’ and ‘inappropriate.’

One financial institution CISO noted: “all threats are insider threats; once a hacker enters the company’s environment, it becomes an insider threat.”

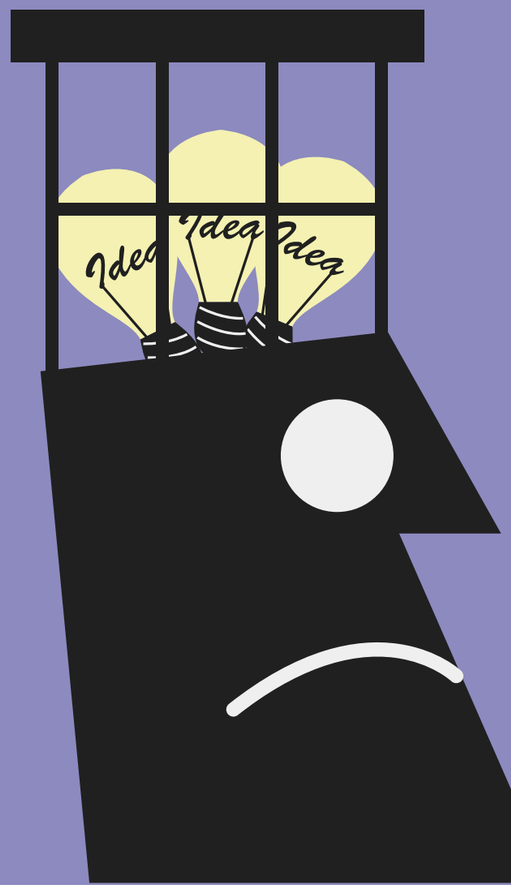
“Not all insider threats are mischievous,” countered another financial institution CISO.

Those nuances characterised many of the other explanations, which varied to include the following simple and complex descriptions:

- A malicious actor who is an internal employee
- People with access to data trying to sneak it out the door
- An internal employee who knowingly or unknowingly grants unauthorised access to someone
- An outside entity trying to get in by taking advantage through social engineering or a relationship to access internal data
- Any user activity that falls outside of the organisation’s policy
- A person who is affiliated with the organisation and through negligence or malice puts the organisation at risk
- The usage of inside systems by authorised and unauthorised individuals in a seemingly nefarious way
- Someone with knowledge of the system who uses that knowledge to create or exploit a weakness.

One insurance executive explained that individuals interpreted ‘insider threats’ according to their roles in the organisation.

“If you speak with individuals in physical security, it could be a disgruntled employee with a weapon,” he said. “For those in finance, it could be an employee with high-level credentials secretly moving money or accessing intellectual property to endanger the company’s competitive landscape.”



Nearly

30%

do not have an insider threat policy or program

Tracking insiders remains elusive

“The overwhelming focus of discussions around cybersecurity relate to protecting money and valuable information,” said Kent. “These are the primary targets for cybercrime and cyberespionage activities; private data and financial information are easily monetised on the black market and often very poorly protected.” Given this sensitivity, almost all respondents (93%) reported being able to identify their critical value data and 100% said they were capable of detecting who retrieved that data.

“All organisations have roles allocated to users of particular data so they can monitor who is accessing it at any time,” said a financial services vice president.

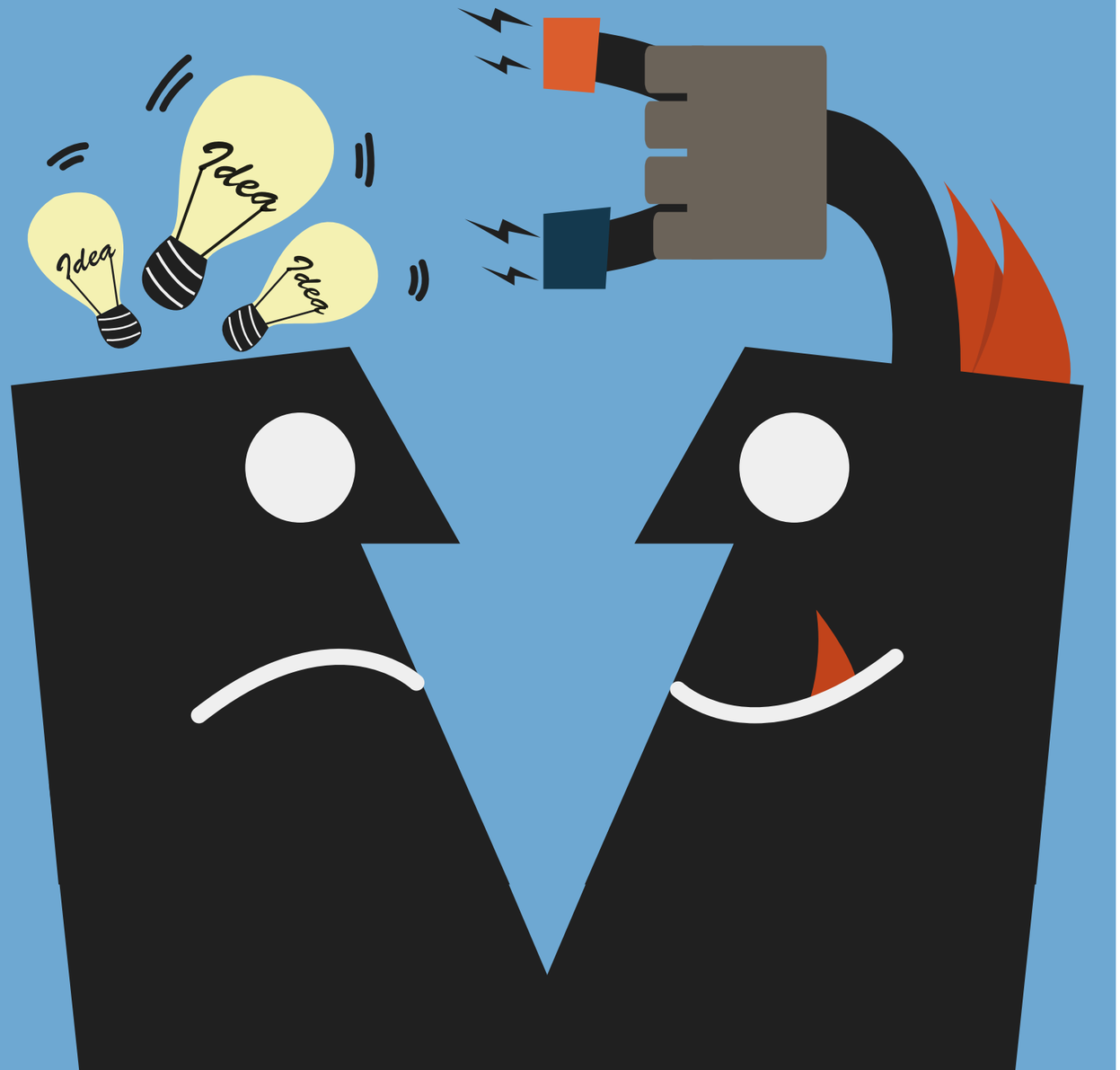
Those numbers fall materially to 69%, however, when asking about whether their organisations know what people do with the critical value data after they access it.

“That is the hard part,” admitted an IT leader in the energy sector.

“The company only knows when data is leaving its network; it is the inside looking out toward the perimeter as information leaves, rather than being maintained within the company’s environment,” explained an information security manager in finance.

46%

are providing actual responses to simulated threats during testing



Data security policies abound, but testing and measuring is a challenge

It is not surprising that so many organisations have insider threat policies because 100% of them already maintain a data security policy, which 64% update annually. Almost all (96%) have an incident response readiness policy (down from 100% in 2014) so the art of documenting protective practices remains widespread.

When asked about gauging the effectiveness of their policies, about a fifth of the respondents said they conducted annual audits. A similar-sized group said they tracked user behaviour and the number of incidents.

“The company’s internal audit group audits against the policy,” said a technology company director.

“The company studies the number of identified attempts to penetrate its system and the lack of success,” added another security director in the entertainment industry.

In terms of testing their incident response programs to ensure compliance with current policies and practices, 18% of respondents said they measured annually. In general, however, most organisations are testing on a more frequent basis; 68% reported engagement in this process multiple times per year, 21% tested twice annually and 32% did so at least quarterly.

More than one-third (36%) engaged in tabletop exercises and 46% provided actual responses to simulated threats. Some applied a combination of both techniques and 11% said they didn’t know what methodology they used.

A large majority (85%) said their incident response team included legal counsel, public relations leaders, and crisis managers, among others in finance and accounting, information technology, compliance, regulatory affairs, risk management, law enforcement, privacy, cyber insurance and physical security.

In addition, 82% have a bring-your-own-device policy, which is a material increase from the 69% of respondents who had one in 2014; 86% permit remote access, down from 96% in 2014.

Humans are the problem … so training remains paramount

Policies and procedures are irrelevant if individuals are unfamiliar with them, or if they are unwilling to adhere to any restrictions. For that reason, it was no surprise that 93% claimed human behaviour was the biggest threat to their organisations' security, up from 88% in 2015.

"The company has increased its budget for training and education; the key is to improve processes and awareness," said one respondent.

"People forget that no matter how much technology you have, it is those using it that are the concern," added another.

As a result, when asked what they found to be the most effective messaging strategy, 39% chose fear over best practices to avoid risk. Fear has grown in popularity as a strategy, up from 31% who selected that option in 2014.

"You always need to have a little fear because it helps for the best practices to be heard," noted an information security manager with a technology company.

"Best practices work best at higher levels of the organisation, but fear is more effective with lower level staff," clarified a security officer with a life sciences company.

The use of fear to educate was not, however, universal, according to an official in the energy sector: "fear is a knee-jerk and go-to reaction, which is unfortunate. "The consensus was that mandatory training, praise for positive action and relevant examples from personal and professional perspectives were the most likely techniques for overcoming inadvertent employee errors.

"Once you get people trained, keeping them trained is easy," added an energy sector chief security officer.

39%

use fear to cut down human mistakes that can lead to threats

The cloud still raises concerns

The number of organisations migrating data to the cloud this year (71%) was consistent with the figures from 2014 (73%), but the number migrating systems to the cloud dropped from 58% to 43%. This decline may reflect the number of organisations that have already migrated data and applications to the cloud.

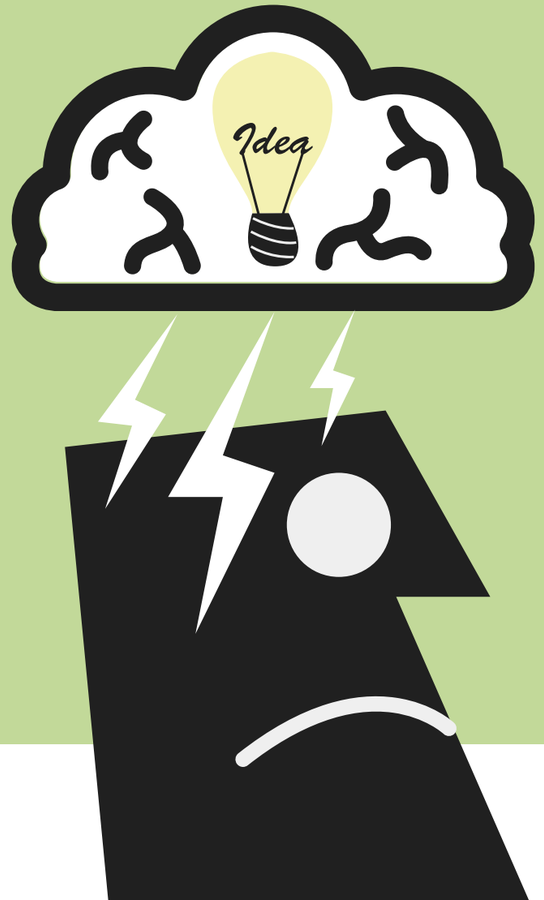
Again, a majority of respondents agree that use of the cloud creates unique cybersecurity concerns (86% in 2015 vs. 84% in 2014).

Those concerns include:

- Losing visibility into the management of your data
- Being at the mercy of the cloud entity's cybersecurity skills
- Reducing control over access to data
- Creating confusion about what happens when the government wants to inspect the data
- Lack of regulatory compliance
- Variations in cloud providers
- Operating in a shared environment.

"Depending on who you are sharing it with, it will limit the ability to perform internal forensics," noted one participant.

"The cloud provider has more sophisticated security than our company," countered another.



86%

agree the cloud creates unique cyber concerns

Reimagining the data breach and potential responses

A quarter of the leaders surveyed said they were not concerned whether their organisations had been breached.

"The smarter CISOs are worried about how to improve protection; it is like worrying about when it will rain because if a breach happens, it happens," said a CISO in the hospitality industry. "I think about how to be better and how to react to a breach more quickly. "Another advised that there was always an element of concern due to the undetectable nature of more sophisticated attacks: "It is like having termites in your house because you don't know what you don't know."

Still, 32% of respondents described themselves as "very concerned" about whether they have been breached.

"It keeps me awake at night," remarked an IT professional with an energy company.

The remaining participants were neither overly concerned nor unfazed by the prospect of a breach.

"You will never be able to stop a breach," said one.

"Even if someone gets through the door, they are not there long enough to cause harm," added another, expressing confidence in the organisation's data segmentation and security practices.

One global director in financial services summarised the consensus: "Any company that says they weren't breached is fooling themselves."

Despite the unified outlook, "people are reluctant to discuss if they are experiencing cyber-attacks or have suffered a data breach – often for fear of showing weakness or giving up a potential competitive advantage," advised Kent. "Even if organisations can overcome their reluctance to talk about security issues, they lack a standard technical mechanism to share, digest and apply anonymised threat intelligence. "Perhaps reflecting a shift in in the direction that Kent suggested, 96% of respondents said they shared and collaborated with other information security executives. This is an increase of four percentage points over the 2014 result.

Within the organisation, 25% of respondents said they interacted with colleagues in eDiscovery, legal, records management and information governance daily, and 100% did so at least monthly.

"Anyone who doesn't collaborate is setting themselves up for failure," said one chief information security officer. "The job of a CISO is collaboration; it requires many hats. What makes a successful CISO is whether the person can sit with the business and talk."

Outlook for 2016

The focus on insider threats will increase

Since about a third of respondents operate without an insider threat program or policy, there is room for this issue to evolve across the corporate landscape. If organisations do not address insider threats proactively, they could be forced to shift by a breach or a lawsuit seeking to assign responsibility for great security.

“If you have not made insider threat protection a priority, the court will force you to do so,” said Lowry noting that litigants are increasingly trying to prove negligence or failure to meet an acceptable standard of care on the part of a data custodian. “Regulators such as the Federal Trade Commission in the US also have the authority to enforce cybersecurity laws, which further complicates the environment. ”To get started, Lowry recommended engaging your organisation’s executives to embrace this challenge.

“Get senior leadership to advocate for insider threat protection and cybersecurity as a priority,” he said. “Grant authority to an individual who is responsible for insider threats and can cross boundaries within the organisation to find them.”

The designee and the program you create must be agile to counter the aggressive nature of the threats that are occurring. “Insiders don’t care about laws or privacy regulations; they will do anything they want,” Lowry explained.

Tolerance for inadvertent security errors will decrease

Organisations will lose tolerance for employees who misunderstand, misinterpret or miscalculate longstanding security policies and procedures. They will begin to penalise careless staff members who invite a breach despite receiving training on the subject. A number of participants highlighted that these consequences could rise to the level of termination.

“There is a recognition now that when it comes to cybersecurity, everyone is responsible, not just those working in IT,” said a financial services leader.

As that perspective proliferates throughout the business community, individuals will feel a shared responsibility to act more thoughtfully in the best interests of the organisation.

“Most employees will not cause a problem out of malice, they are typically just ignorant,” said a life sciences executive.

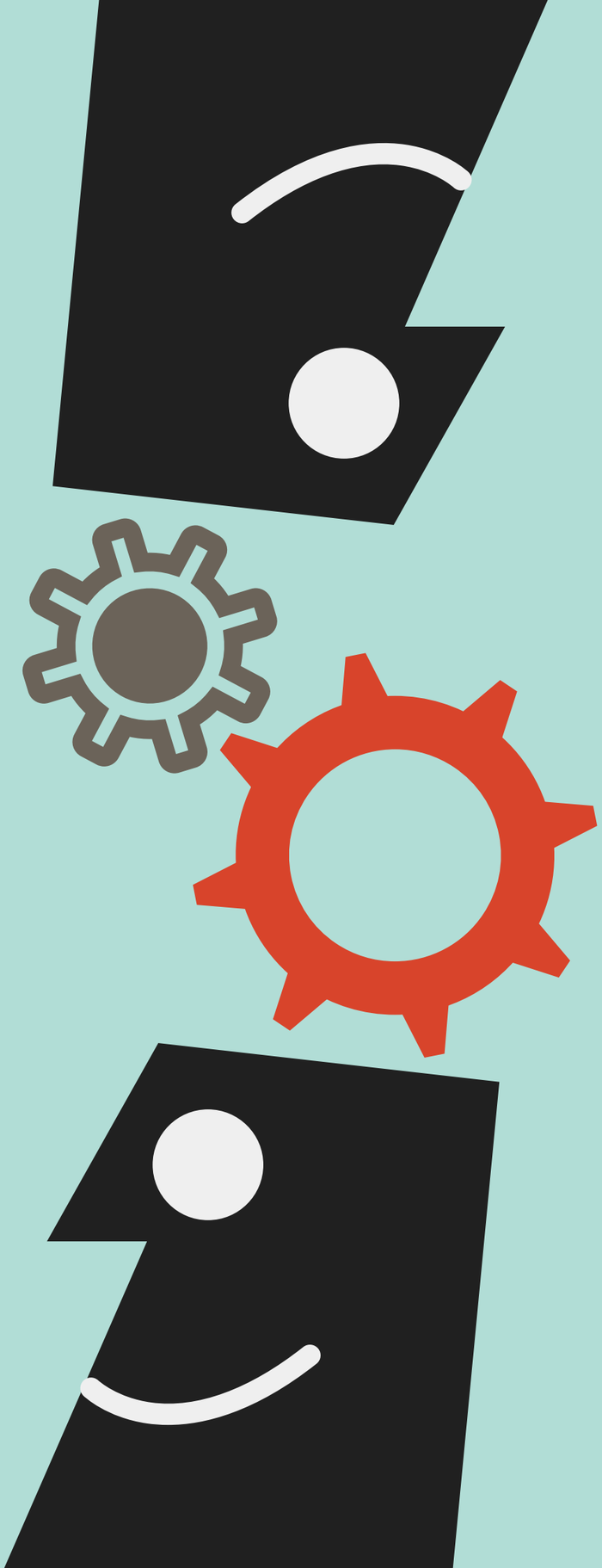
Cybersecurity will continue to be an influential company concern, rather than solely an it issue

The issue of information security has taken the highest priority within most organisations, virtually equivalent to profitability, corporate governance and staffing. It is a critical concern that has sweeping implications beyond what anyone may have anticipated a decade, or even a few years ago. “If you don’t take good cybersecurity care, you may have your S&P score downgraded, which could have a huge economic impact,” commented Lowry.

As a result, the profile of the security team and its leadership is likely to rise. In addition, the influence of the CISO will grow throughout the C-suite, similar to the way the general counsel’s weight has risen over the years.

25%

interact with peers in their organisation daily



Technology will evolve as a partner in the cybersecurity battle

Most people believe technology, improved processes and educating users have a roughly equal role in preventing data breaches. Respondents to this year’s survey rated technology and improved processes at about 30% each and education at about 35%.

“While I have controls in place, if the controls are effective and social engineering is showing the correct process, things can still occur despite having the best technology,” said one manager of security at a manufacturing company.

“You could have the greatest technology and processes, but if your employees do not know what to do, they could open the wrong door to trouble,” added a director in financial services.

Kent highlighted that new forms of technology would help organisations build stronger protocols and encourage greater employee awareness.

“We need to move away from the ‘green type on black screens’ model of technology and deliver answers in a more accessible and digestible format,” he said. “We must let technology to do the hard work for us and enable smart people to use their brain power and analytical skills more effectively.

Nuix

Nuix protects, informs and empowers society in the knowledge age. Leading organisations around the world turn to Nuix when they need fast, accurate answers for investigation, cybersecurity incident response, insider threats, litigation, regulation, privacy, risk management and other essential challenges.

Nuix makes small work of big data volumes and complex file formats. Our solutions combine advanced technology with the extensive knowledge of our global team of industry experts. We bring data to life with clarity and intelligence to solve critical business problems, reduce crime and secure and manage information.

North America
USA: +1 877 470 6849

» Email: sales@nuix.com

EMEA
UK: +44 207 877 0300

» Web: nuix.com

APAC
Australia: +61 2 9280 0699

» Twitter: @nuix

nuix
Simple. Powerful. Precise.