KPMG

Fighting cyber with cyber

Deep learning threats demand deep learning solutions

kpmg.com

A new era of cyber threats and cyber security

Researchers have long pondered the ever-proliferating amount of information with which we are bombarded and how we can most efficiently manage, store, understand, and utilize it.

Every day, every hour, every second, individuals, companies, and governments generate and share vast quantities of facts, opinions, figures, and statistics. And the volume is expanding exponentially. Data—big and small, structured and unstructured—is inescapable and essential.

And it's under siege.

Credit reporting agencies, health care organizations, financial services providers, social media and email platforms, electrical grids, transportation systems, our elections—no corner of the economy is insulated.

With the rapid growth of cloud-based and open source applications, cyber security has taken center stage in virtually every industry.

These innovations and a host of others have created a new risk matrix, placing greater priority than ever on deterrence and protection. Consider that a business experiences a ransomware attack—think "WannaCry," which locked down computers in more than 150 countries in 2017—every 40 seconds, and is expected to increase to every 14 seconds by 2019.[1] Deputy Attorney General Rod Rosenstein has characterized ransomware as "a new business model for cybercrime."[2]

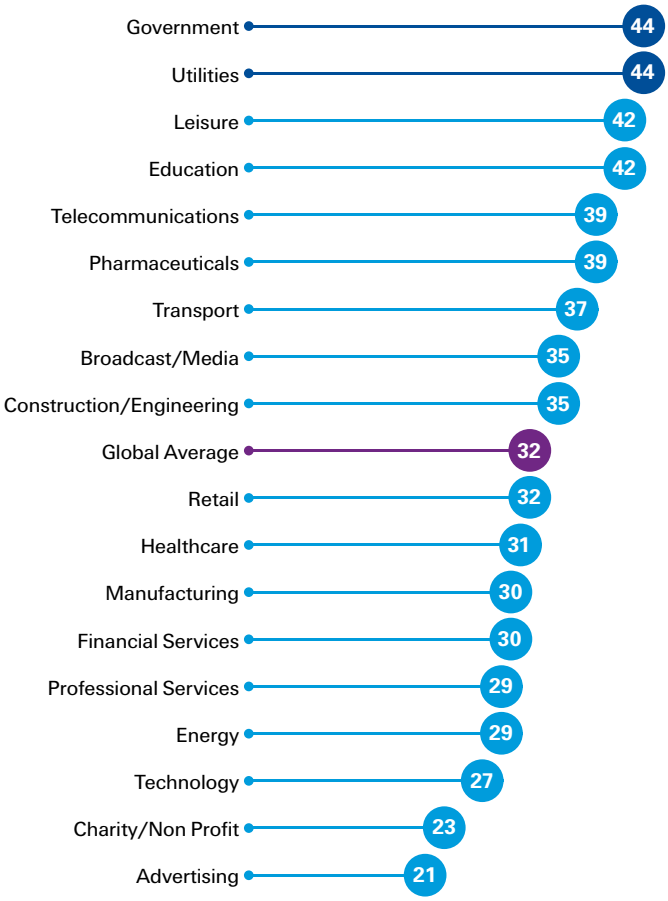
Unfortunately, most legacy IT infrastructures were not designed to meet the demands of this new environment and many companies are struggling to adapt, not just in terms of architecture and tactics, but also with internal controls and policies.

Security professionals are exploring cognitive technologies and artificial intelligence, particularly deep learning, to better anticipate and defend against cyber threats. Bad actors are implementing the same tools to increase the sophistication of their attacks. The good guys need to stay a step ahead.

1 Source: Cybersecurity Ventures, "Official 2017 Annual Cybercrime Report" (October 19, 2017).

2 Source: From remarks at the Cambridge Cyber Summit (October 4, 2017).

Cyber attacks in high-target sectors show utilities and government at most risk



Values in percentages

Source: Harvey Nash/KPMG CIO Survey 2017

Drowning in data

The increasing vulnerability of personal, corporate, and government information places a new urgency on cyber security. Consider the growth of the Internet of Things. According to Intel, there will be 200 billion wireless smart devices by 2020, up from 2 billion in 2006.

This explosion in the number of connected devices boosts productivity, collaboration, and drives innovative thought, but it also escalates the potential breach points.

Microsoft Azure AD, a cloud-based active directory for managing identity and access, has millions of accounts and sees billions of logins every day. No human, or group of humans, can reasonably make sense of that much data, mine it for patterns, and look for threats and vulnerabilities with consistent speed and precision.

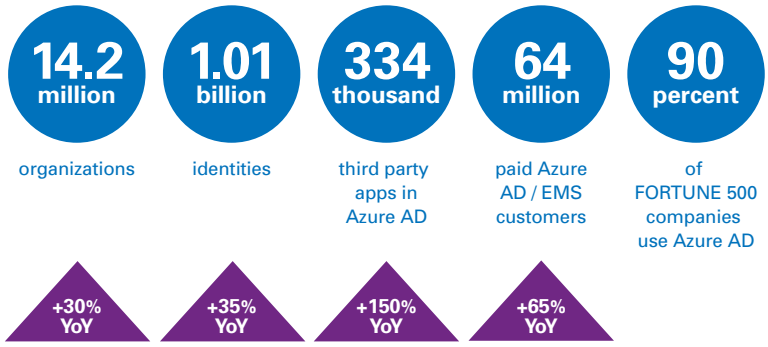
The pace of change has been so rapid that security advances have not adapted fast enough. There is login data, customer interaction information, transactional data—basically, event-based data from across the entire enterprise. How can you prevent, detect, and respond to security incidents while also using that data to provide actionable insights to your business partners?

Cyber security professionals need to be able to go back to their business partners and say, "Based on the data we're observing, these are the things you should be aware of and protecting against." The issue extends beyond IT and cyber security. It's a business imperative for the entire supply chain.

Many companies are wrestling with this in connection with the small amount of experienced data talent they have on staff. Organizations are spending so much time and energy thinking about how to spread around the few engineers and data scientists they have that the goal of developing and deploying a flexible, targeted cyber security plan has largely gone unfulfilled.

We are seeing a significant shortage of data scientists and specialists across virtually every industry. As a result, we see most businesses deploying this talent—to the extent they have it—to solve myriad business problems, rather than working on critical cyber security use cases, such as anomaly detection.

Every Office 365 and Microsoft Azure customer uses the Azure Active Directory—whether they realize it or not

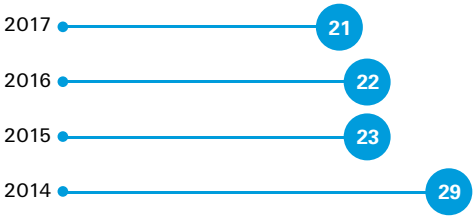


Source: Microsoft 2018

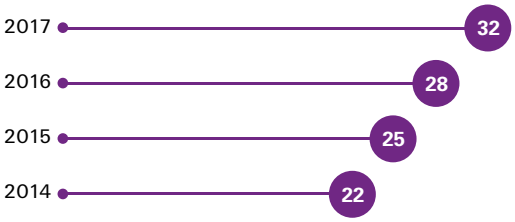
Security in the spotlight

With all the promise of advancements in artificial intelligence—new solutions in genomics and medicine, safety, and transportation—there are darker implications. That same technology is also available to bad actors looking to mislead, destroy, and steal.

Confidence among CIOs in their organization's cyber preparedness is steadily declining…)



… while the number of serious attacks is increasing.



Values in percentages

Source: Harvey Nash/KPMG CIO Survey 2017

The threats are becoming more sophisticated, and current cyber defenses are not enough. According to the Harvey Nash/KPMG CIO Survey 2017, 89 percent of CIOs are actively investing in digital innovations, but only 21 percent feel well-prepared in terms of cyber security. Not surprisingly, more than half (52 percent) are devoting increasing budget dollars toward technology platforms and tools designed to help the organization predict, detect, and combat threats.

It's a definite concern and major challenge, but it's also an opportunity for security professionals to partner with their organization's IT group and CISO. This ensures the entire enterprise understands and is positioned to manage the risks while realizing the benefits of automation and cognitive advances.

Security leaders have an obligation to identify and protect the organization's "crown jewels"—key business processes, intellectual property, enterprise and customer data, and market offerings. This process is complicated by automation-related risks that were previously nonexistent.

Historically, cyber security began as a somewhat passive endeavor (firewalls, antivirus software, malware protection). But with more than 250,000 new malware strains emerging daily[3] and 60 percent of mid-sized organizations across 10 countries agreeing their current defenses are insufficient,[4] today the focus is evolving to include proactive, adaptive prediction.

Hackers and other bad actors are discovering and attacking system weaknesses that may be a decade or more old. These vulnerabilities must be addressed. For many organizations, it comes down to a lack of talent/manpower, time, budget, or understanding of the nature of the threats—typically it is a combination of these challenges.

3 Source: AV-TEST, The Independent IT-Security Institute (March 1, 2018).

4 Source: Sophos, "The State of Endpoint Security Today" (January 2018).

Deep learning: Bright promise, dark risks

One strategy security professionals are exploring more and more to address today's ever-growing threats centers on artificial intelligence techniques—deep learning in particular.

The conventional wisdom has long been that computers learn best by following logical, deterministic rules. As technology progressed, researchers, principally University of Toronto computer scientist Geoffrey Hinton, explored a simple proposition: that computers could learn like the human brain—using intuition, rather than rules.

This notion became the groundwork for deep learning, which is a subset of machine learning, in which the machine is trained by numerous data inputs to make probabilistic predictions, rather than being programmed by humans.

Also referred to as "neural networks," deep learning identifies and learns from patterns, much like some processes in our brains, which organize information across an intricate network of neurons that communicate across cortical pathways. Deep learning employs layered neural networks to quickly recognize abstractions in large volumes of often unstructured data and make precise assessments.

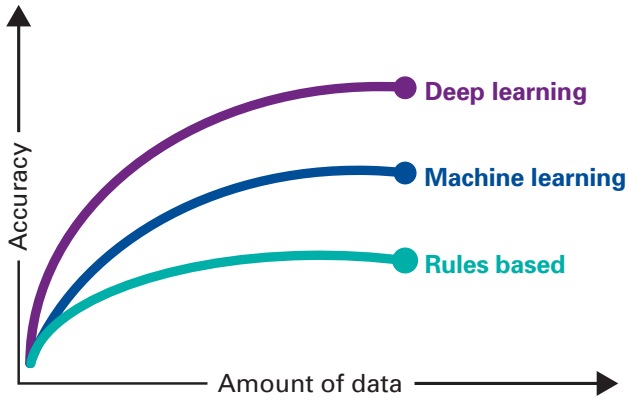
The fascinating and frightening thing about the deep learning branch of artificial intelligence is that it can enable the machine to learn without human supervision. More complex perhaps is that, just as we don't truly understand how the brain works, often we are unable to determine how exactly neural networks learn to do what we want or, even more troubling, how it learns to do the opposite.

A multi-layered neural network defines its own pattern and, depending on the sophistication of the application and the programmer, makes decisions and executes solutions on the fly. At a high level, this explains how deep learning powers autonomous vehicles. The car takes action based on an interpretation of its surroundings and the behavior of everything around it.

From a cyber security perspective, deep learning as a technique is evolving to be smarter and more adaptive, but there remain limitations, particularly in relation to how these systems manage unpredictability. It may still be something of a black box, but we're only at the beginning of this story in terms of threat detection and deterrence, but the optimism around deep learning appears to be well founded.

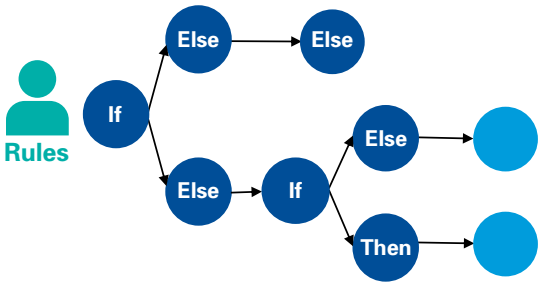
Deep learning takes advantage of large data sets to learn and improve over time

A deep learning system's output becomes more accurate as it receives more data. Deep learning utilizes a set of analytical layers, where each successive layer performs more generalizable learning tasks until a pattern is identified. This work is performed in fractions of seconds.



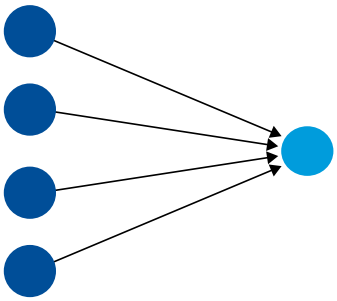
Rules based

– Humans define all connections and paths between input and output



Machine learning

– Humans define the features that represent possible connections from input to output, but machines learn the optimal path



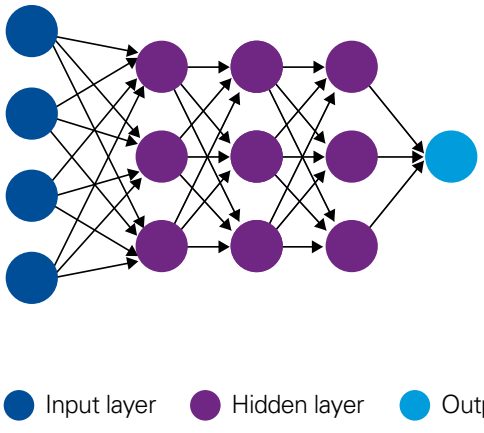
Deep learning

– Subset of machine learning where hidden layers represent non-human created paths from input to output

– To learn how to make correct decisions, the hidden layers attempt to generalize, at increasing levels of complexity, over input features

– These layers are referred to as "hidden" simply because they are in neither the input nor the output layers

– Currently, the generalizations made by the hidden layers are not directly interpretable by humans



Source: KPMG Cognitive Automation Lab 2018

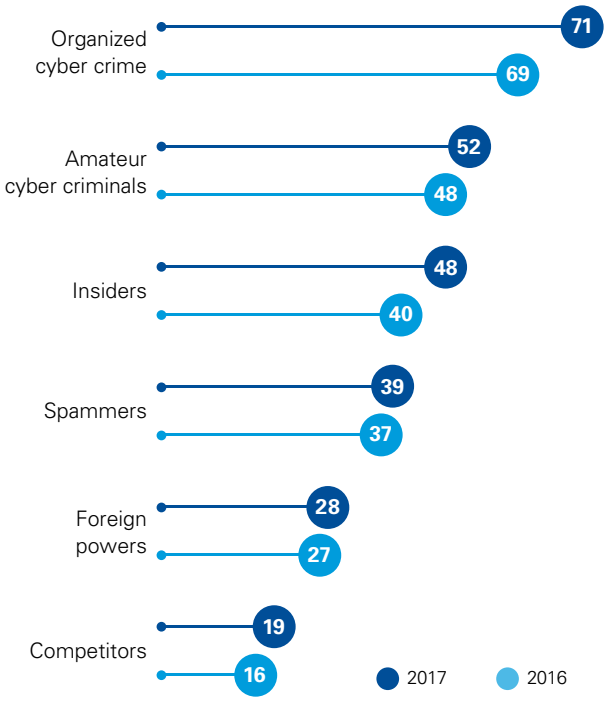
Combat deep learning threats with deep learning solutions

The applications for deep learning are invaluable and seemingly limitless across the global economy, with examples ranging from brain cancer detection and weather forecasting to energy usage fluctuations and autonomous vehicles. The fact that Google, IBM, Facebook, Twitter, and Salesforce have all acquired deep learning start-ups over the past several years is testament to the potential viability of this field.

However, artificial intelligence-powered threats must be on your radar. While 62 percent of cyber security professionals surveyed at Black Hat USA 2017, a leading information security conference, expect cyber criminals to ramp up their attacks using artificial intelligence over the next year, 32 percent said they do not expect artificial-intelligence-related attacks. This is surprising and a bit troubling.

How are bad actors getting their hands on such cutting-edge algorithms? There is an API economy forming. These advanced technologies are now largely accessible to anyone with a credit card via the cloud. Artificial intelligence APIs are on full display, and they can do virtually anything, from face and speech recognition to predictive modeling and sentiment analysis. Because of this broad accessibility, the emerging concern is that this technology may become a tool not only for legitimate, well-intentioned individuals, companies and organizations, but also for organized crime, terrorist groups, rogue nations, APTs, lone wolf hackers, and others.

Bad cyber actors come in many forms—threat origins that CIOs are most concerned about



Values in percentages

Source: Harvey Nash/KPMG CIO Survey 2017

There are numerous ways these applications can be weaponized for malicious purposes, from penetrating databases to steal personal and corporate data and intellectual property to creating large-scale automated phishing campaigns. The technology can even change video to make minor variations to facial expressions that can alter the intent of the footage, but are otherwise undetectable. These schemes are incredibly difficult to defend against.

Bottom line, we believe it will take deep learning solutions to combat deep learning threats. In this sense, cyber security could ultimately be a key differentiator for enterprise IT innovation.

Security professionals have historically dealt with the challenge of "making sense" of the data they collect to shore up their defenses. Deep learning has the ability to correlate numerous data sources to identify patterns or anomalies that might point to malicious activities. Companies are employing deep learning algorithms not only to help them identify security incidents, but to assess system-wide vulnerabilities. As a self-learning technology, deep learning offers the prospect of adaptive improvement as organizations strive to produce positive cyber security outcomes.

Protection through detection

As a cyber security tool, deep learning has been making particular progress in three areas:

Adversarial sample detection

This is a particularly interesting example because it demonstrates the use of deep learning itself to take on one of its biggest weaknesses, wherein false samples are introduced to make the system behave in an inappropriate or misleading manner. Research suggests that hidden neural layers can be activated to detect incorrect classifications caused by adversarial attacks. [5]

Malware detection

While that research is still relatively new, much of the work has been focused on more typical cyber security areas such as malware detection. Most malware detection systems have required hybrid use of both standard machine learning and deep learning because the feature space has been much too large for deep learning to appropriately handle. However, recent advances demonstrate that in some cases, full deep learning approaches are better able to classify malware once it has been identified. [6]

Network intrusion detection

Finally, network intrusion detection has long been a problematic area because of the requirement to predict what is essentially unpredictable. In the past few years, deep learning approaches have begun to outperform previous state-of-the-art methods for academic data sets, and while results remain relatively low, the promise of deep learning to either bolster traditional approaches or provide a possible unsupervised approach is apparent. [7]

5 Source: N. Papernot, et al., The Limitations of Deep Learning in Adversarial Settings (2016).

6 Source: B. Kolosnjaji, et al., Deep Learning for Classification of Malware System Call Sequences (2016).

7 Source: B. Dong, et al., Comparing Deep Learning Method to Traditional Methods for Network Intrusion Detection (2016).

Think pragmatically—there are a lot of touch points

The key for senior security leaders and systems analysts across the corporate and government sectors will be to move from being reactive to being proactive and adaptive.

They must be mindful of the overall architecture of their networks. As mobile and the cloud expand as enterprise options, data is changing hands more and more, increasing the risk of breaches. It is critical to consider the security implications at every touchpoint.

How do organizations make their information ecosystems adaptive? There's a lot of learning that needs to happen on a continuous basis. The ability to contemplate large data sets, make inferences, and then apply that thinking to your security model is a full-time job, and, in a big data world, the limitations of the human brain become exposed quickly.

The data ecosystem is broad and deep—you must approach security holistically.

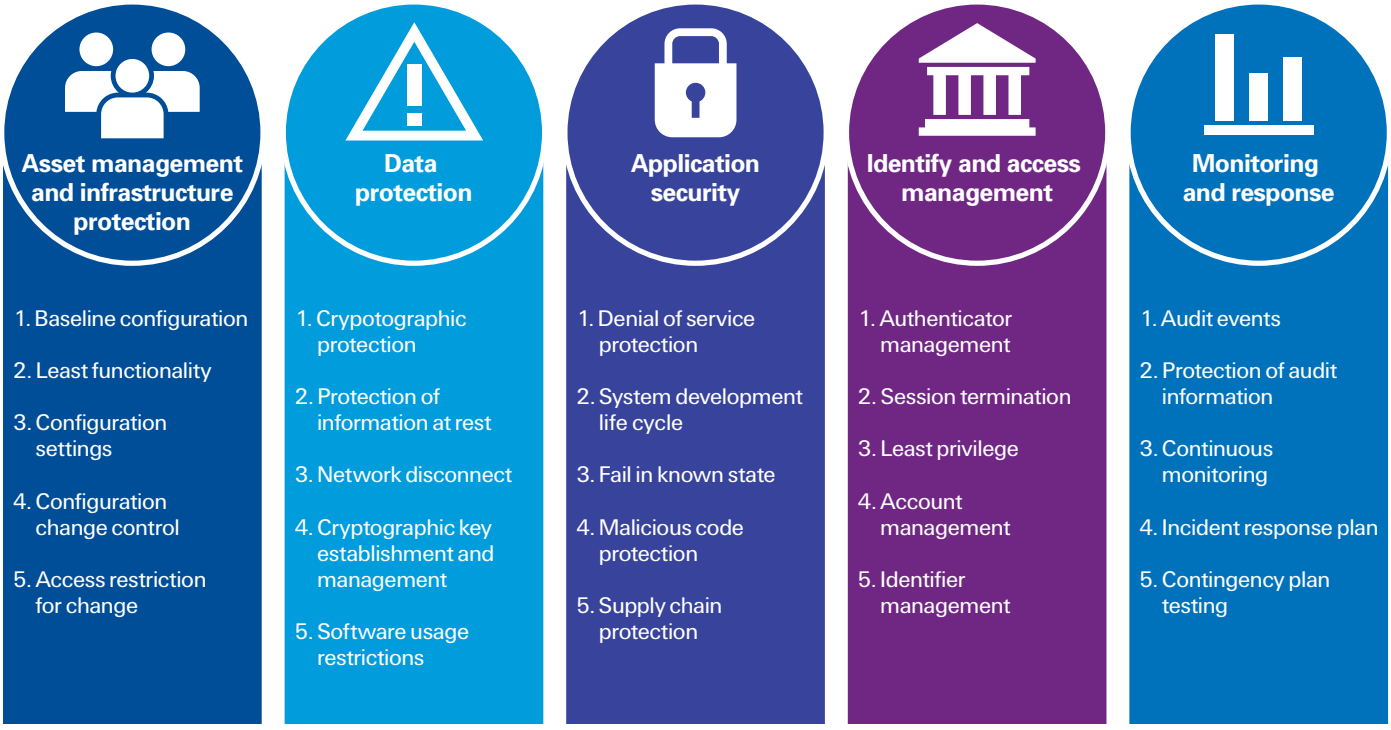
In this dynamic environment, the only way to have a solid cyber defense is to have an adaptive cyber security framework that reacts and responds to changes proactively. To that end, we have identified five basic cyber security risk categories that apply to artificial intelligence solutions. By thinking about AI risk broadly and holistically, organizations will be best positioned to respond to whatever specific threats emerge.

While the risk categories will look familiar to most cyber security or IT professionals, the specific strategies for addressing them in the context of AI may not. To that end, we have further broken down these risks into more than 80 customizable targeted controls. These controls apply good security practice to the specifics of intelligent automation and have been further classified per their applicability at the foundational level or specific to the technology solution being applied.

For example, in terms of data protection, special focus needs to be given to information used to train machine and deep learning solutions, because corruption of training data can lead to breakdowns in the algorithms being deployed.

Similarly, the infrastructure within which these bots or algorithms are executed also need to be managed to prevent runtime "botjacking" wherein "man-in-the-middle" type attacks can expose the risk of a rogue administrator hijacking a run-time session for malicious activities.

KPMG cyber security risk framework for AI



Source: KPMG 2018

Next steps: where do we go from here?

Deep learning represents an opportunity for organizations to augment and build out security capabilities to protect, enable, and sustain the business.

KPMG encourages CEOs and CISOs to make cyber security and next-gen solutions like deep learning a primary element of the overall strategic business plan.

While much about these technologies is new, the approach for improving security capabilities is familiar. Organizations need to have a coordinated enterprise cyber security blueprint that looks out over the next three to five years. This framework should incorporate every touchpoint; include strategies for infrastructure, data science talent, internal controls, governance, and must have the flexibility to accommodate changes, as developments inside and outside the organization demand.

We suggest starting with this strategic plan:

Set your security risk profile and policy

1. IA security risk and capability gap assessment
2. Establish policies
3. Target state architecture
4. Technology rationalization
5. Target state organization and process
6. Implementation roadmap

Build a framework to manage cyber risks

1. Security solution selection to address capability and risk gaps
2. Agile design and implementation of process and solutions
3. Organization and governance changes
4. Integration with existing solutions and processes

Monitor and improve your security controls

1. Define and implement operational processes
2. Configure and tune detection and alerting thresholds and policies
3. Perform one-time and ongoing audits
4. Ongoing IA security and risk assessments

Effective cyber security incident response

1. Design process, technology, and people changes to help ensure appropriate response for IA incidents
2. Conduct triage and forensics response processes

Incident recovery, awareness, and learning

1. Design and implement resilience and recovery measures for critical systems and data
2. Help ensure ongoing learning and improvement
3. Conduct awareness training

Source: KPMG 2018

Conclusion: There is no silver cyber bullet

There are no definitive answers, no cut-and-dried solutions. We're in a new era of cyber threats and cyber security. Perhaps as much as it takes groundbreaking technologies, it requires talent—data scientists, cyber strategists, cognitive engineers, robotics experts—thinking critically, asking questions, and gathering insight.

Areas of greatest investment in technology expected in three years

61% **Data analytics**

58% **Cognitive technologies**

55% **Internet of things**

Source: KPMG U.S. CEO Outlook 2017

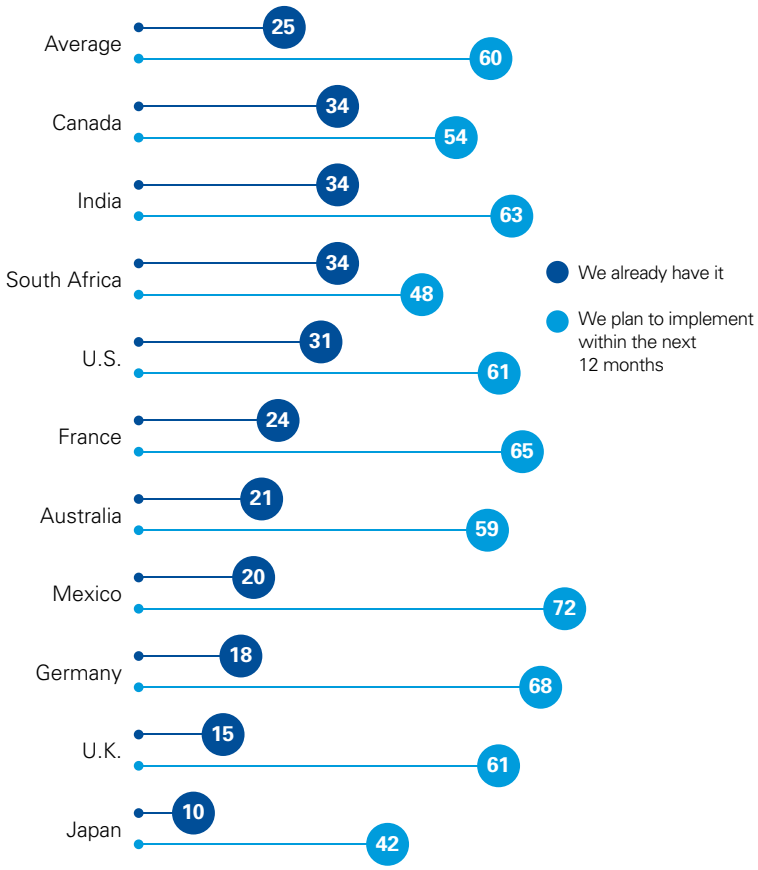
The wide-ranging promise of artificial intelligence and techniques such as deep learning is truly exciting. However, the technology underlying these advances is now also available to those who would use it for mischief and worse.

That's the blessing and the curse: adaptive, intelligent bots can learn to do remarkably precise and reliable work designed to illuminate or deceive.

From an enterprise perspective, the questions in relation to artificial intelligence, machine learning, and deep learning are around augmenting existing systems to improve and respond to these threats and malicious software attacks in a near-automated fashion.

In general, security organizations have lagged in their ability to predict, detect, and respond to threats in an automated manner. This is where the power of deep learning systems can be leveraged to ensure that cyber security systems have the ability to continually learn and improve their defense mechanisms. The key for security professionals is understanding—and keeping up with—the pace and speed at which cybercriminals are using these tools.

Organizations worldwide that have or plan to add predictive threat technologies to their cyber security arsenals



Values in percentages

Source: Sophos, *The State of Endpoint Security Today,* 2017

How KPMG can help

Our intelligent automation capabilities were built to help our clients unlock the value of AI to accelerate their strategies for automation and cost management, growth and customer engagement, and risk and regulatory policy. Together with our clients, we leverage intelligent automation across the full spectrum of the value chain, creating solutions that are transforming business and operating models.

Cyber security is a strategic enterprise risk that goes far beyond IT. Whether we are working with your boardroom, back office, or data center, we seek to provide a jargon-free explanation of your cyber threats, the potential impact to your critical assets, and the recommended response. Ultimately, we view cyber security through a cross-functional business lens, encompassing people, change, financial, and risk management.

About the authors

Cliff Justice

Principal, KPMG LLP, Innovation & Enterprise Solutions

Cliff is a principal in KPMG's Innovation & Enterprise Solutions team, leading the firm's cognitive automation initiatives. As a leading authority on global service delivery model design and sourcing, he has more than 25 years of experience in operations, technology, outsourcing, offshoring, and business transformation. Cliff has been an early leader in applying intelligent automation, robotics, and cognitive technologies to business operations and services.

Steve Barlock

Principal, KPMG LLP, Cyber Security Services

Steve is a principal at KPMG and a senior business and technology leader with 25 years of experience in consulting related to IT strategy and delivery. With a broad technology background, Steve has deep specialization over the last 15 years in information security and its application in a business context.

Anurag Rai

Director, Cyber Security Services and Risk Management, Compliance and Privacy Leader, KPMG LLP

Anurag is an acknowledged leader in information security, risk management, compliance, and identity and access management (IAM) domains. Anurag's certifications include C|CISO, CISSP-ISSAP, CISA, CISM, and CRISC.

Contact us:

Cliff Justice
Principal
KPMG Innovation & Enterprise Solutions
713-319-2781
cjustice@kpmg.com

Steve Barlock
Principal
KPMG Cyber Security
415-963-7025
sbarlock@kpmg.com

Anurag Rai
Director
KPMG Cyber Security
312-665-2563
anuragrai@kpmg.com

To discover more of KPMG's insights on cognitive automation, robotic innovations, the digital workforce, and how to keep it all protected, please visit:

kpmg.com/us/intelligentautomation

kpmg.com/us/cyber

kpmg.com

kpmg.com/socialmedia

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.