Cybersecurity in the cognitive era

Priming your digital immune system

IBM Institute for Business Value

How IBM can help

Cybercrime is an insidious threat that has reached crisis levels. Though hard to quantify with precision, estimates of the cost of cybercrime to the global economy range from USD 375–575 billion per year. No geography or industry is immune. IBM has a broad, integrated portfolio of security software and services that address prevention, detection, response and remediation to help organizations anticipate and take early action to mitigate the impacts of cybersecurity risks. IBM Security helps clients establish a security immune system backed by analytics, real-time defenses and proven experts. To learn more about how IBM works with organizations to secure their digital infrastructures, please visit **ibm.com**/security.

New capabilities for a challenging era

Security leaders are working to address three gaps in their current capabilities — in intelligence, speed and accuracy. Some organizations are beginning to explore the potential of cognitive security solutions to address these gaps and get ahead of their risks and threats. There are high expectations for this technology. Fifty-seven percent of the security leaders we surveyed believe that it can significantly slow the efforts of cybercriminals. The 22 percent of respondents who we call "Primed" have started their journey into the cognitive era of cybersecurity — they believe they have the familiarity, the maturity and the resources they need. To begin the journey, it is important to explore your weaknesses, determine how you want to augment your capabilities with cognitive solutions and think about building education and investment plans for your stakeholders.

Executive summary

The state of cybersecurity is reaching an inflection point. The number of risks and events is growing exponentially, and security operation teams are struggling to keep up with the volume. The threat landscape is changing rapidly, with the sophistication and numbers of threat variants becoming too great to stay abreast of, using traditional approaches. The repercussions of incidents and breaches are increasing, with the financial costs and risks growing rapidly. Finally, many organizations are faced with a dearth of security experts with the right skills. All of these different stresses make it difficult for organizations to maintain the healthy digital immune systems they need to protect themselves.

For this report, we surveyed 700 chief information security officers (CISOs) and other security leaders from 35 countries, representing 18 industries. Our goals were to uncover what these leaders are challenged with, what their shortcomings are and what they are doing about them. We also wanted to understand their views on cognitive security solutions — how these leaders think the solutions could help, the extent of their readiness to implement and what might be holding them back.

We found that security leaders are challenged by the complexity of threats and the speed with which they are able to respond to them. They are worried about how security incidents affect their operations today and how they may shape their reputations tomorrow. Security leaders don't feel they are as effective as they could be in addressing network and data protection and rapid, intelligent threat response. However, they are looking to address these deficiencies in the next few years. Acquiring the right resources to tackle these issues will be difficult. Faced with increasing costs and a shortage of skilled security resources, security leaders are looking for ways to better justify their investments to business leaders.

The **primary cybersecurity challenge** today and tomorrow is **reducing average incident response and resolution times**.

57% of security leaders believe that **cognitive security solutions** can significantly **slow the efforts of cybercriminals**.

There is expected to be a **threefold increase** in the number of professionals **implementing cognitive security solutions** over the next 2–3 years.

As organizations gather more security data and apply more analytics capabilities, the increases in workload are reaching the limits of what's possible through manual means. There are some who are looking to cognitive security solutions to manage this situation and help address gaps in intelligence, speed and accuracy. Even though cognitive technologies for security are in their early days, there is great hope and optimism about their potential. Our survey respondents said that the top benefits they expect from cognitive-enabled security solutions are improved detection and response decision-making capabilities, significantly improved incident response times and increased confidence when discriminating between events and true incidents. Despite the great promise, there is still a lot of education and preparation that has to happen before widespread adoption occurs.

We did find a group that was "primed for the cognitive era" of security solutions. When we looked at security effectiveness, cognitive readiness and understanding, we identified enthusiastic security leaders who feel they are ready to enter the cognitive era of security solutions today. In general, these leaders tend to have a better familiarity with cognitive solutions, a higher overall confidence in their security capabilities and fewer challenges with attaining resources.

As cognitive security solutions become more established and widespread, any organization will be able to tap into their benefits. If you feel you are ready and decide to begin the journey, the first step is to identify what weaknesses you hope to address using cognitive security solutions. Next, learn about potential use cases and match them with your weaknesses. In an environment where investment justification is expected, spend time communicating the benefits of cognitive security solutions to your business stakeholders. Emphasize, in business language executives will understand, that these solutions can improve your overall security posture. By taking these early steps, you are priming your organization for the cognitive era of cybersecurity.

The current context

When scratching the surface of the current cybersecurity landscape, you might get the impression from the security leaders we surveyed that the situation is manageable. In fact, these professionals have faith and confidence in their growing technological and organizational capabilities. A majority — 77 percent — of those we asked about cybersecurity preparedness feel that they are on par with their industry peers. The respondents are also very optimistic about their cybersecurity posture over the next 2–3 years, with 86 percent saying they will be *better* positioned than their industry peers.

These responses might not be surprising, but it is important to examine them: Security leaders believe they aren't doing worse than anyone else and have confidence that they are making progress and will continue to make progress. Almost three-quarters think they are effective in addressing the foundations of organizational security, with 72 percent saying they are effective at IT hygiene and 71 percent saying they are effective at risk awareness across their company. But let's drill down a level to see what is really happening with challenges, impacts, capabilities, funding and return on security investments.

The need for speed

The number one challenge for security leaders today is reducing average incident response and resolution times. Forty-five percent of respondents identified these times as a top cybersecurity challenge today. Organizations don't see this challenge going anywhere over the next 2–3 years. Looking to the future, 53 percent of respondents believe that improving responsiveness will remain a top cybersecurity challenge (see Figure 1).

"It's literally like being a merchant sailor in the golden age of piracy — there is no navy to protect you, there is no police force, you are on your own. On top of that, many don't know how to sail their boats, and they can't fire back at the attackers (it's illegal). You are literally trying to survive in a hostile world with both arms tied behind your back. However, you do have some really interesting and sophisticated tools to use that tell you all about your threats."

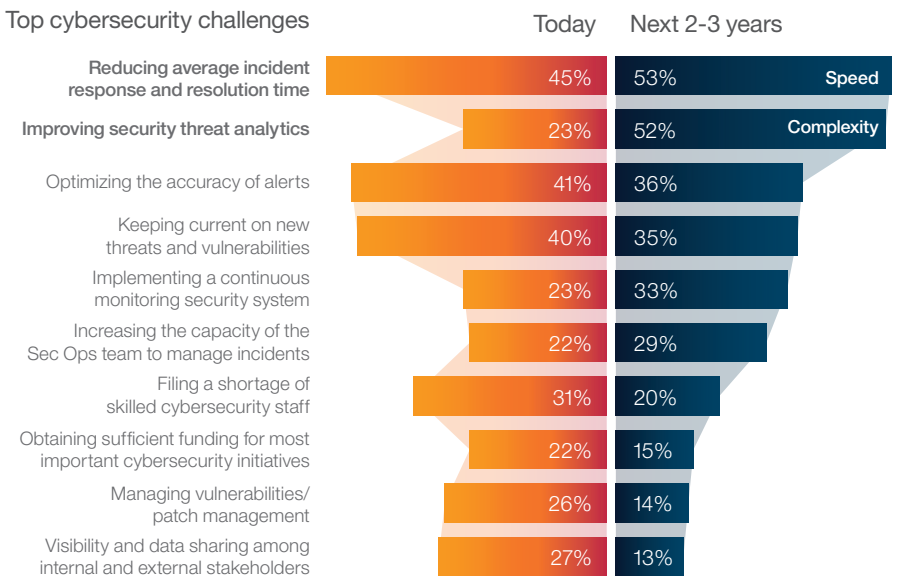
David Shipley, Director of Strategic Initiatives, Information Technology Services, University of New Brunswick

Time equates to greater risk

In a 2016 study, the Ponemon Institute discovered that the time required to identify a breach averaged 201 days and the time required to contain a breach averaged 70 days. The institute also determined that utilizing an incident response team was the single biggest factor in reducing the cost of a data breach.[1]

Figure 1

Security leaders identified the top cybersecurity challenges today and what they think the challenges will be in the near future



These concerns persist despite the fact that 80 percent of organizations tell us their incident response speeds are much faster than they were two years ago (on average 16 percent faster). Eighty-six percent want their speed improvements to be even faster over the next 2–3 years (with an average improvement goal of 24 percent faster).

This is an extremely important matter for organizations. The longer an organization takes to respond to an incident, the greater the damage it may sustain and the more money it may lose dealing with the crisis. Time most definitely heightens the risk of loss.

Another growing challenge for security leaders is around improving security threat analytics. Twenty-three percent of those we surveyed identify this as a top challenge today, but 52 percent expect improving security threat analytics to be the primary cybersecurity challenge over the next 2–3 years. Security analysts need help gathering knowledge, determining which threats are the most pressing and looking quickly for patterns and deviations in activity. Security leaders will be searching for anything that can help improve their speed and manage the complexity of the threats they face.

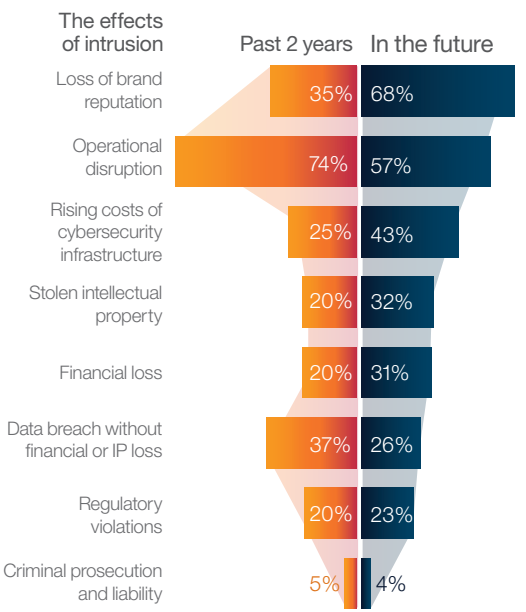
Widening worries

Nearly three-quarters of those we surveyed said that intrusions resulted in significant operational disruptions over the past two years. However, what respondents expect over the next few years is dramatically different.

Companies are increasingly concerned that intrusions will result in a loss of brand reputation in the future — overtaking operational disruptions. Concern about loss of reputation nearly doubles as respondents look to the future, with 35 percent identifying this as a result over the past two years but 68 percent worried about it in the years to come (see Figure 2). This shift shows that many security leaders fear the expanding effects of intrusions. Increasingly, the consequences are not just about operations, but reputation; a tarnished reputation can drag down revenue as trust wanes and customers turn away.

Figure 2

Organizations reported a variety of ramifications stemming from intrusions over the past two years but expect the consequences to shift in the future



The rising cost of cybersecurity infrastructure also becomes a more substantial issue in the future, increasing dramatically from today. As the risk from successful intrusions persists, organizations default to spending more money to solve the problem. Security leaders often assume that if they suffer an intrusion something is to blame, so they look to upgrade people, point solutions and infrastructure to stay safe.

Security shortcomings

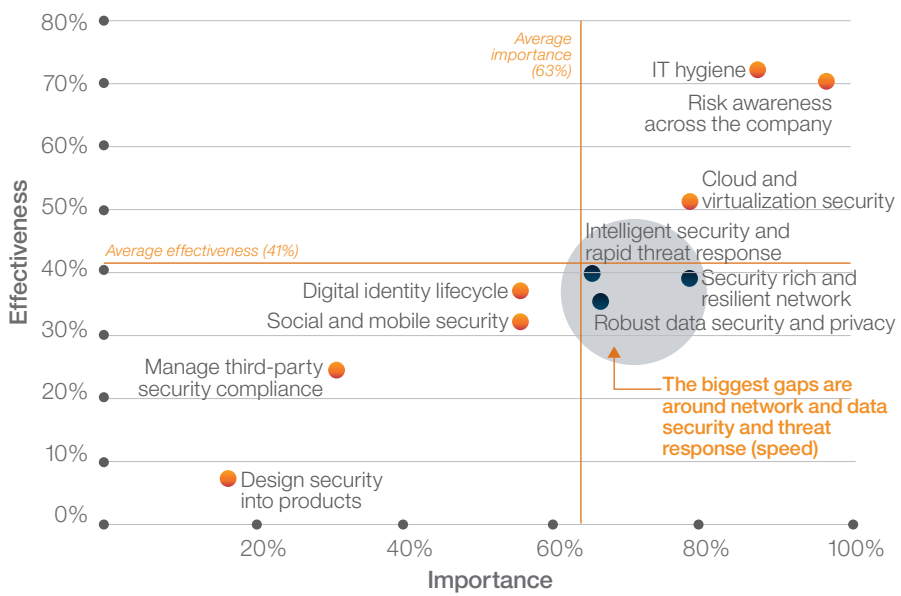
We asked respondents across a wide variety of security capabilities what they think is important to their security posture and what they believe they are effective at. Security leaders generally feel they have to treat almost everything as important, because they don't want anything to slip through the cracks. However, with limited resources, no one can be on the cutting edge of all areas all the time, especially when new technologies, approaches and challenges are emerging continually.

Most respondents said they are comfortable with how they are handling IT hygiene and managing risk awareness across the company — the basics from both a technological and an organizational standpoint. The areas that respondents think are important, but that they are ineffective in addressing, are the ones we want to examine (see Figure 3). Network and data protection coupled with threat response fall into this category.

Respondents said they aren't as effective as they need to be when it comes to their threat response speed, security information event management (SIEM), network activity detection, filtering, and data classification and loss prevention. Of course, it is vital that organizations stay ahead of the increasing volume and complexity of security risks; by focusing on their response speeds and managing complexity through better threat analytics, organizations can bolster their defenses significantly.

Figure 3

The importance versus effectiveness of various security capabilities



"We have uncovered a number of tangible cost savings across the enterprise that originated from our security monitoring and analysis. We have reduced bandwidth costs, decommissioned low utilization resources and increased employee productivity by significantly reducing spam, to name a few."

A Canadian leader in financial protection, wealth and asset management

Managing the balance sheet

Security leaders have a tremendous amount they need to focus on. They also anticipate large increases in the costs of effective cybersecurity, and they don't see these expenses decreasing anytime soon. Seventy-eight percent have seen the cost for cybersecurity increase over the past two years, and 84 percent expect it to continue to increase over the next 2–3 years. In fact, more than 70 percent of respondents spend more than 10 percent of their entire IT budget on cybersecurity (with the majority spending between 10 and 15 percent). These expenditures go mostly to prevention and detection. On the extreme end, we have seen financial institutions spending upwards of USD 500 million annually on cybersecurity.[2] Because more money doesn't necessarily guarantee more protection, this rise isn't sustainable in the long run — security leaders are going to be under increasing pressure to justify their investments.

Ninety-two percent of respondents say their funding requests for cybersecurity initiatives require an ROI or other financial analysis for justification and approval. As part of this justification, the top two factors used to justify investments include clear communication of the current risk exposure in the organization (according to 61 percent of respondents) and getting the support from finance, risk management, operations and other key executives (according to 51 percent of respondents). Security leaders have to communicate their needs in the language of the business and ensure they have the support of other key executives.[3] Going forward, they must look for new ways to justify the cost of cybersecurity investments and show value. The view that security is simply an insurance policy or a cost of doing business must be dispelled.

Dealing with deficiencies

The good news is that the security leaders we surveyed seem to be aware of their shortcomings and are planning on addressing them in the near future. Organizations are pursuing a number of different initiatives to improve their cybersecurity risk preparedness (see Figure 4). Today's efforts mainly center on improving employee behaviors though education and training — with 67 percent of organizations pursuing these avenues. Forty percent of respondents are also implementing identity monitoring software. These options would generally be seen as more fundamental.

Figure 4

The initiatives security leaders are pursuing to improve cybersecurity risk preparedness

Rank today		Rank in 2-3 years	Initiatives
1	▼-30%	5	Improve employee behaviors through education and training
2	▼-25%	7	Implement identity-monitoring (user activity) software
3	▲+8%	4	Report on operational / strategic security measures with new analytics tools
4	▲+28%	1	**Improve monitoring of network, application and data-level security**
5	▲+17%	3	**Improve incident response methodology, processes and response speed**
6	▼-9%	8	Hire and train more security analysts
7	▼-16%	10	Application security testing (including mobile, API)
8	▲+36%	2	**Build out or refresh SOC capabilities**
9	▲+14%	6	Implement cognitive-technology-enabled security solutions
10	▲+1%	9	Incorporate forensics capabilities into security operations

"Executives are growing weary of throwing lots of money at security, with no positive feedback that all the previous spending has made them that much safer. Security leaders need to go further to justify investments — don't just do an assessment, identify gaps and then ask for money to close those gaps."

Chad Holmes, Principal and Cyber-Strategy, Technology and Growth Leader (CTO) at Ernst & Young LLP

Over the next 2–3 years a large shift in these improvement initiatives is expected. In fact, respondents indicated that the top three initiatives will be completely different than today's. Number one will become improving network, application and data-level security, with 57 percent identifying. Building out or refreshing SOC capabilities will be number two. Finally, improving incident response speed will become the new number three. All of these areas correspond with the effectiveness shortcomings identified earlier.

It's good to see security leaders addressing their shortcomings, but significantly changing priorities may create new gaps, or widen existing ones. No matter what, security leaders should make sure they are addressing what is most relevant to the business. The real question is whether these expected future efforts will be enough.

Exposing the gaps

All of these challenges, weaknesses, efforts and pressures highlight three critical gaps — in intelligence, speed and accuracy. Security leaders must address these gaps while simultaneously managing cost and ROI pressures.

Intelligence gap

- The most challenging area due to insufficient resources is threat research, according to 65 percent of respondents.
- Forty percent of respondents say that keeping current on new threats and vulnerabilities is a significant cybersecurity challenge.

Speed gap

- The top cybersecurity challenge today and tomorrow is reducing average incident response and resolution times — despite the fact that 80 percent say their incident response speeds are much faster than two years ago.
- Respondents expect to increase their focus in this area in the coming years. Only 27 percent say they have current initiatives to improve incident response, but this will increase to 43 percent over the next 2 – 3 years.

Accuracy gap

- According to respondents, the second most challenging area today is optimizing accuracy alerts (there are currently too many false positives).
- Sixty-one percent of respondents say another significantly challenging area due to insufficient resources is threat identification, assessing threats and knowing what potential incidents to escalate.

The most-cited benefits expected from a cognitive security solution

1. Intelligence
Improve detection and incident response decision-making capabilities

2. Speed
Significantly improve incident response times

3. Accuracy
Provide increased confidence to discriminate between events and true incidents

3x increase in planned adoption of cognitive security solutions in the next 2-3 years

How will cognitive security be used?
Cognitive systems will be used to analyze security trends and distill enormous volumes of structured and unstructured data into actionable knowledge. Security leaders and analysts can't possibly absorb all the human-generated security knowledge that is out there, including research documents, industry publications, analyst reports and blogs. Cognitive systems look to blend that information with more traditional security data. Cognitive security solutions will be used in combination with automated, data-driven security technologies, techniques and processes — helping to ensure the highest levels of context and accuracy.

Cognitive security solutions can help augment the capabilities of SOC analysts — helping them to increase the speed of their response, better identify threats, strengthen application security and reduce the overall level of enterprise risk. The goal is to move analysts away from the mundane, repetitive security tasks to the most intellectually challenging work.

Enter cognitive security solutions

To close the gaps, different technologies and approaches are needed. Organizations can't simply spend or hire their way to their goals over the long term. As security technologies have evolved over the years, they have moved from simple perimeter controls (such as focusing on static defenses) to more advanced security intelligence capabilities (such as focusing on real-time information and deviations from patterns).

Today, we are beginning to enter the cognitive era of security — defined by solutions that can understand context, behavior and meaning by analyzing both structured and unstructured security data. Cognitive security looks to unlock a new partnership between security analysts and their technology. These solutions can interpret and organize information and offer explanations of what it means, while offering a rationale for conclusions. They also learn continuously as data accumulates and insights are derived from interaction.

The benefits of cognitive security solutions
Imagine a set of solutions enabled by cognitive technologies, allowing you to:

- Enhance the capabilities of junior SOC analysts by giving them access to best practices and insight that used to require years of experience.
- Improve your response speed by applying external intelligence from blogs and other sources, so you can take action before signatures are available.
- Quickly identify threats and speed detection of risky user behavior, data exfiltration and malware infections using advanced analysis methods.
- Gain greater context around security incidents through automation of local and external data gathering and reasoning.

The promise and challenges

Many of those we surveyed believe that the benefits of cognitive security solutions will address the gaps they are facing. Even though cognitive security is an emerging technology area, 57 percent believe that cognitive security solutions can significantly slow the efforts of cybercriminals — they see the promise and potential benefit.

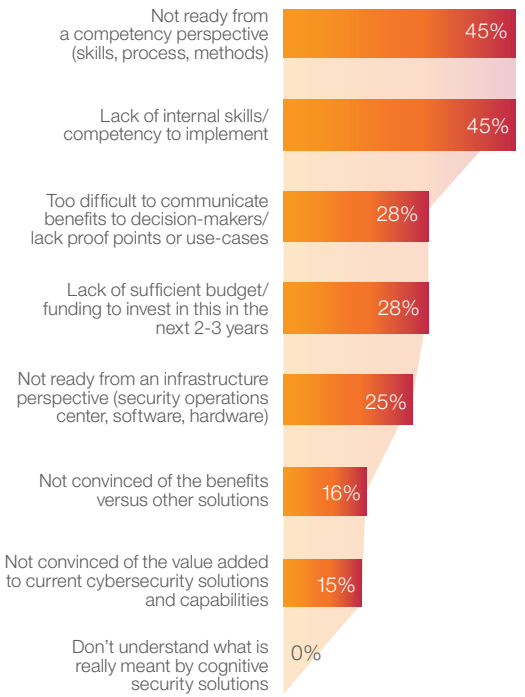
When we asked security leaders to select the benefits of a cognitive-enhanced security solution, 40 percent cited improved detection and incident response decision-making capabilities, 37 percent pointed to significantly improved incident response time, and 36 percent said increased confidence to discriminate between events and true incidents. Respondents want cognitive security solutions to be able to address their major gaps. They need these solutions to help with intelligence, speed and accuracy.

Today, only seven percent of those we surveyed are working on implementing cognitive-enabled security solutions to improve cybersecurity risk preparedness. This is expected since the capability is so new. However, in the near future the number of those looking to implement these solutions rises threefold, to 21 percent. Over the next few years we will see accelerated adoption as security leaders add this capability to enhance their digital immune systems.

Respondents did see potential challenges to the adoption of cognitive security solutions. It is not that security leaders don't understand the technology conceptually or aren't convinced of the value or the benefits versus other solutions; the challenges are more about skills, processes and methods. Forty-five percent of respondents said that the top adoption challenges are not being ready from a competency perspective and a lack of internal skills to implement (see Figure 5). To allay these concerns, more education and preparation needs to happen.

Figure 5

Security leaders identified the top challenges with implementing cognitive security solutions



"We are poised to take the next step with cognitive and intelligent solutions that will efficiently ingest, organize and bring context to an enormous amount to security information and knowledge which today consumes a lot of our time and resources."

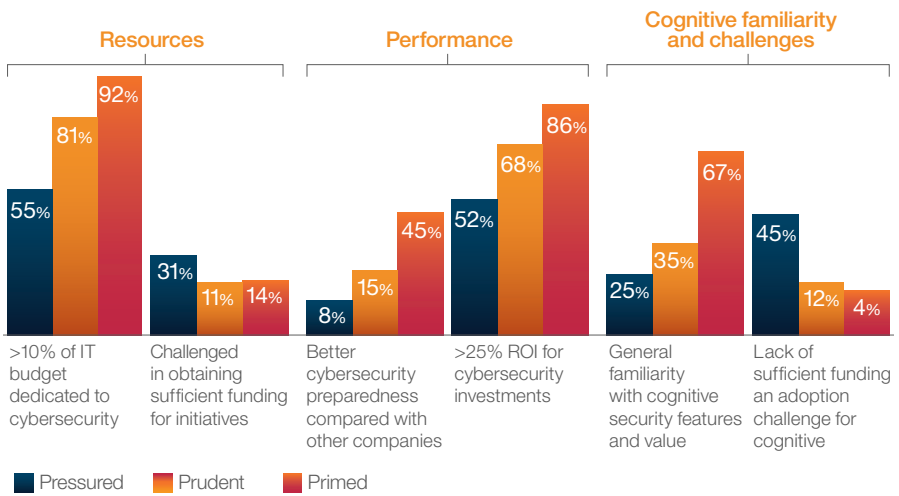
A Canadian leader in financial protection, wealth and asset management

Primed for the cognitive era

To understand who is ready to leap into the cognitive era of security today, we profiled our respondents based on their self-described level of security effectiveness, cognitive understanding and readiness. An analysis of their responses revealed three distinct clusters (see Figure 6).

Figure 6

Pressured, Prudent and Primed organizations characterize their preparedness



The *Pressured*, which make up 52 percent of our sample, are characterized by funding and staffing challenges and a lower general familiarity with cognitive security features and value. They generally have a lower percentage of IT budget allocated to cybersecurity and are more likely to report challenges with obtaining sufficient funding and addressing staff shortages. They also cited a lack of sufficient funding as an adoption challenge for cognitive. (For details

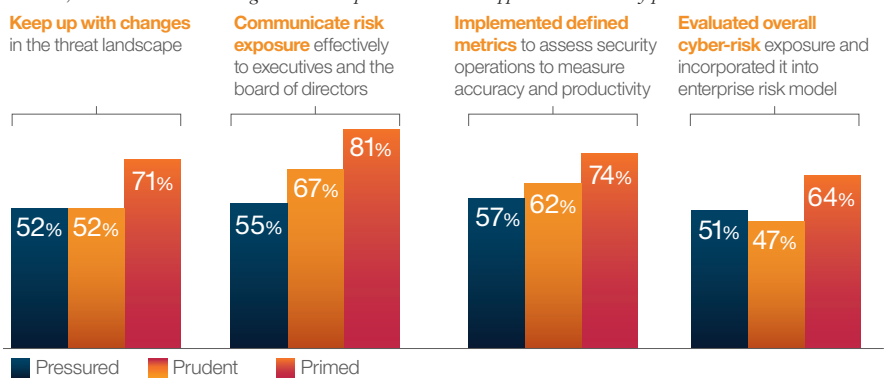
about how we established and defined these clusters, see the "Demographics and methodology" section on page 20.)

The *Prudent*, which make up 27 percent of the sample, don't have the same resource challenges as the Pressured, but they aren't as fully ready to implement next-generation cognitive enabled security today.

The *Primed*, 22 percent of the sample, are the most knowledgeable and enthusiastic about cognitive security solutions. The Primed have a better familiarity with cognitive security and higher confidence, budget and ROI than the others. They believe they employ a more mature approach to their security practices, with a higher percentage saying their security operations team is able to keep up with changes in the threat landscape. They effectively communicate risk exposure to their executives and boards of directors, and they incorporate cyber-risk exposure into their enterprise risk model (see Figure 7).

Figure 7

Pressured, Prudent and Primed organizations report their various approaches to security practices



"There is a massive amount of noise out there; the human brain can't process everything on a day-to-day basis. We need something to help, something like AI or cognitive technologies."

Chad Holmes, Principal and Cyber-Strategy, Technology and Growth Leader (CTO) at Ernst & Young LLP

"The 24/7 nature of security operations presents a challenge that is costly for most organizations to staff, which is where the appeal of cognitive-enabled security comes in — it never sleeps or fatigues."

Michael Pinch, Chief Information Security Officer, University of Rochester

What do security leaders expect and want from cognitive security solutions as they begin their pursuit? In conversations with those who are Primed, we found they wanted cognitive security solutions that could:

- Always be on, providing continuous support
- Help reduce false positives and find anomalies in behavior
- Better understand the threat landscape and provide context to incidents
- Support governance, risk management and compliance — based on unique industry, geography and other regulatory requirements
- Change the nature of security work, helping analysts to work smarter and provide a higher level of value

It's to be expected that security leaders who feel they are more mature and have fewer resource constraints would be the first to explore an emerging technology like cognitive security. However, it is important to realize that everyone, with additional knowledge and experience, can apply cognitive technologies to address their shortcomings and extend the limits of their analysts to improve security operations.

Recommendations

We explored the current security landscape in order to understand the pressures, challenges and priorities of our respondents. Based on what we observed, we have compiled recommendations to help you and your organization become primed for the cognitive cybersecurity era.

Recognize your weaknesses

Security leaders want to increase their responsiveness and reduce complexity, and they are increasingly concerned about a loss of reputation as a consequence of incidents. Look at the primary weaknesses and vulnerabilities within your organization. How are they connected? What is a priority?

- Are you lacking the intelligence and threat research you need?
- Are your incident response and resolution times fast enough for your operations?
- Are you having trouble discriminating between events and true incidents, or putting things into proper context?

Become educated about cognitive security capabilities

Take a holistic and formal approach to learn about cognitive security solutions. There could be many misconceptions in your organization from a capability, cost and implementation perspective.

- Understand the potential use cases for cognitive security solutions — match them to your areas of weakness. Do you want greater context for security incidents, better evidence to improve decision making or new ways to proactively assess risk?
- Plan for how you can communicate the benefits of cognitive security solutions to technical and business stakeholders — build an education plan for your team and your executives.

"Cognitive security has so much potential—you can meet your labor shortage gap, you can reduce your risk profile, you can increase your efficiency of response. It can help you understand the narrative story. People consume stories—this happened, then this happened, with this impact, by this person. Additionally, cognitive can lower the skills it takes to get involved in cybersecurity. It allows you to bring in new perspectives from non-IT backgrounds into cracking the problem."

David Shipley, Director of Strategic Initiatives, Information Technology Services, University of New Brunswick

- Identify and address skills gaps that may hold back adoption of the technology within your own organization.

Define an investment plan

It is difficult to build an investment case when a technology is new and unproven in the market — you don't have many examples to point to, and building trust can be difficult. Since the vast majority of our respondents said their funding requests require an ROI or other financial analysis, it is imperative that security leaders take a different approach to cognitive security solutions.

- Treat cognitive security solutions as something distinct. Don't just focus on traditional security investment justification, such as cost to fix. Instead, focus on the fact that cognitive security is a capability that can improve the overall effectiveness of security operations.
- Take the education plan you develop and use it to achieve buy-in from other executives in the business, and get them to help make the investment case.
- Think creatively and look for novel ways for your investment in cognitive security to help the business, besides only ROI.

Look to augment your capabilities, no matter your maturity

Those we identified as Primed tended to have more resources available to them, more confidence in their capabilities and a readiness to implement cognitive security solutions today, but this doesn't mean cognitive security is only for a select group. Cognitive security solutions are an emerging technology area, and its unique characteristics can benefit organizations of all sizes.

- *If you are Pressured:* Identify specific business measures and skill shortages that cognitive security solutions could help improve, then build the investment case.
- *If you are Prudent:* Focus on getting well informed to lessen the anxiety around skills gaps.
- *If you are Primed:* Channel your enthusiasm, pick a very specific use case for a cognitive pilot implementation and make sure it is not isolated from your broader security operations.

For more information

To learn more about this IBM Institute for Business Value study, please contact us at iibv@us.ibm.com. Follow @IBMIBV on Twitter, and for a full catalog of our research or to subscribe to our monthly newsletter, visit: **ibm.com**/iibv.

Access IBM Institute for Business Value executive reports on your mobile device by downloading the free "IBM IBV" apps for phone or tablet from your app store.

The right partner for a changing world

At IBM, we collaborate with our clients, bringing together business insight, advanced research and technology to give them a distinct advantage in today's rapidly changing environment.

IBM Institute for Business Value

The IBM Institute for Business Value, part of IBM Global Business Services, develops fact-based strategic insights for senior business executives around critical public and private sector issues.

Contributors
Lisa van Deth, Program Marketing Manager, Campaign & Thought Leadership Strategy, IBM Security; Christophe Veltsos, Associate Professor, Department of Computer Information Science at Minnesota State University, Mankato.

Acknowledgments
Caleb Barlow, Vice President, WW Portfolio Marketing, IBM Security; Maria Battaglia, CMO, Resilient, IBM Security; Wangui McKelvey, Director, Portfolio Marketing - Security Services & Web Fraud, IBM Security; Kevin Skapinetz, Director of Strategy, IBM Security; Oxford Economics, for assistance with administering survey data collection.

Notes and sources

1 "2016 Cost of Data Breach Study: Global Analysis." Ponemon Institute. June 2016. http://www-03.ibm.com/security/data-breach/

2 Friedman, Gabe. "JPMorgan Chase Atty: Bank Will Spend $500M on Cyber Security." January 29, 2016. https://bol.bna.com/jpmorgan-chase-atty-bank-will-spend-500m-on-cyber-security/. Accessed on September, 21, 2016.

3 Kelley, Diana and Carl Nordman. "Securing the C-suite: Cybersecurity perspectives from the boardroom and C-suite." IBM Institute for Business Value. 2016. ibm.biz/csuitesecurity

Demographics and methodology
To better understand what security challenges organizations are facing, how they are addressing these challenges and how they view cognitive security solutions and their potential, the IBM Institute for Business Value (IBV) and Oxford Economics surveyed a balanced distribution of 700 CISOs and other security professionals in 35 countries, representing 18 industries between May and July of 2016.

In order to determine our clusters (the Primed, Prudent and the Pressured) we applied a k-means clustering algorithm that revealed three distinct behavior patterns. These behavior patterns were based on questions relating to security effectiveness, cognitive understanding and cognitive readiness.

About the authors
Diana Kelley is the Executive Security Advisor (ESA) at IBM Security and the manager of the IBM Security Newsroom. As ESA she leverages her 25-plus years of IT security experience to provide advice and guidance to CISOs and security professionals. She has contributed to the IBM X-Force report and frequently publishes thought leadership pieces on the Security Intelligence blog. She is a current faculty member with IANS Research and serves on the Advisory Board for InfoSec World and the Content Committee for the Executive Women's Forum. Diana is a frequent speaker at security conferences and has been quoted as a security expert in *The New York Times, TIME*, MSNBC.com, *Information Security* magazine and *The Wall Street Journal*. She co-authored the book *Cryptographic Libraries for Developers*. Diana can be contacted at drkelley@us.ibm.com.

Vijay Dheap is a Program Director in the IBM Security Division who specializes in graduating emerging technologies into commercial offerings. He currently leads a portfolio of offerings in Security Intelligence that span Advanced Analytics, Cognitive and SaaS. Previously, he led the cyber-forensics and mobile security businesses. Vijay is a technologist at heart and has held the title of IBM Master Inventor. His patent portfolio spans mobile, enterprise collaboration and security innovations. He earned an international MBA from the Duke Fuqua School of Business and a master's in computer engineering from University of Waterloo, Canada. Vijay can be reached at vdheap@us.ibm.com.

David Jarvis is the Security and CIO Lead for the IBM Institute for Business Value. He is responsible for developing and executing an agenda that explores emerging business and technology topics for those areas. He is a passionate expert in the development and management of market insights, thought leadership and strategic foresight projects, and has held multiple positions at IBM in those areas. He is the author of numerous cybersecurity thought leadership reports, including the 2012 – 2014 IBM CISO Assessments. In addition to his research responsibilities, David teaches on business foresight and creative problem solving. David can be reached at djarvis@us.ibm.com.

Carl Nordman is the Global Director of the C-suite Study Program and the CFO Research Lead for the IBM Institute for Business Value. He is responsible for conducting primary research in both domains. He leads studies to uncover current trends and perspectives on current strategic issues. Carl has over 25 years of experience in Finance Risk and Fraud. Previously he has held positions in IBM's Consulting Services practice, delivering engagements for CFOs at Fortune 1000 companies, and running Finance and Accounting BPO services as an Account Executive for several clients. Carl can be contacted at carl.nordman@us.ibm.com.

Route 100
Somers, NY 10589
Produced in the United States of America
November 2016

GBE03779USEN-00