

# THE MEANING OF SECURITY IN THE 21st CENTURY

Understanding root causes of security threats—  
and steps companies can take now



Sponsored by





# Contents

About the report	2
Introduction	3
Executive summary	4
Assessing the security challenge	6
Converging physical and cyber security risks	8
Identifying the hurdles to corporate involvement	9
Moving toward responsive leadership	11
Approaching insecurity battlegrounds: identifying vulnerable areas	13
Education matters	14
Cooperation and collective action	16
Joint efforts in early stages	18
Conclusion and takeaways	20

# About the report

This global study, conducted by the Economist Intelligence Unit (EIU) and sponsored by Palo Alto Networks, sheds light on the ways business leaders are dealing with the increasing volume of threats they face from insecurities that arise because of disruption beyond their corporate borders.

In November 2016, the EIU surveyed 150 board members and C-suite executives in a wide variety of functional roles, from business development to operations to strategy; about half the respondents work in companies with global annual revenues exceeding \$500m.

To complement the survey, the report draws on detailed desk research and in-depth interviews with the following senior executives and specialists (listed alphabetically by organisation):

- Kelly Bissell, managing director, Accenture Security
- Matthew Devost, co-founder, FusionX LLC; managing director, Accenture
- Troels Oerting, chief security officer, chief information security officer, Barclays Plc

- Graeme Newman, chief innovation officer, CFC Underwriting Ltd.
- Henry Shiembob, chief security officer, Cognizant Technology Solutions
- Arvind Parthasarathi, co-founder and CEO, Cyence
- Kevin Hyams, head of the Governance, Risk and Compliance group at Friedman LLP
- Robert Coles, chief information security officer, GSK Group
- Mohamed Alkady, founder and president, Hart Inc.
- Robert Anderson, head of the cyber security practice, Navigant Consulting Inc.

We would like to thank all interviewees for their time and insight. None of the experts interviewed for this report received financial compensation for participating in the interview programme. The report was written by Robert Dieterich and edited by Rebecca Lipman.

The EIU bears sole responsibility for the content of this report. The findings do not necessarily reflect the views of the sponsor. ■



# Introduction

This research begins with the premise that corporate leaders' efforts to manage security risks—threats to physical assets, IT infrastructure and personnel—will be more effective when informed by a clear understanding of those risks' societal motivators.

Executives and board members recognise that sources of conflict—such as ethnic or religious differences, poverty and income inequality, hunger and resource scarcity—motivate many of the insecurity risks they face, a global survey conducted by The EIU reveals. They also acknowledge that such concerns will mostly remain beyond the scope of a corporate security programme. The survey reveals that attempts to address these larger underlying issues might run contrary to corporate culture, demand resources a company doesn't have or risk political pushback. Survey respondents are confident in the abilities of political authorities in relation to these matters, but believe some of the risks to businesses are not given

sufficient political attention.

In the face of these challenges, corporate security leaders explain that their work in this realm mostly occurs at some more actionable middle ground between their standard security measures and the societal roots of the threats. They primarily treat the symptoms, but with the knowledge that in the long run they will need to achieve more.

Today, security-management programmes focus on protection of networks, data and intellectual property, as well as facilities and people. Enhancing cyber security lies at the heart of this effort, with physical security having, in significant ways, converged with digital protection efforts.

Interviewees identified many areas where co-operative action and a growing awareness can help to address the societal motivations that result in security threats, benefitting not only businesses but also society as a whole. ■

# Executive summary

As executives and programme managers survey the spectrum of security issues that endanger their businesses, they face a complex and shifting landscape. The motivations behind these threats are even more complex.

It is standard protocol for companies to construct their best defences to protect their cyber and physical borders, employees, data and more. Security efforts are also generally characterised by their defensive, or responsive, measures; plans to better respond to threats in real time. But corporate leaders are beginning to understand that they might play a role in a third approach—a proactive or preventative, one that can reduce or eliminate the issues that give rise to threats in the first place.

This mission has its fair share of challenges, as many virulent issues like poverty and political tensions are largely beyond companies' control. Nonetheless, businesses leaders agree they should—and can—think beyond the traditional horizons of their security efforts. They see an opportunity to work together to help address issues in the outside world, which would alleviate the threats that manifest inside their companies.

## Key findings

*Causes of insecurity are ever better identified and understood; opportunities emerge to address them for the benefit of the wider business community.*

- **Widespread social issues present business risk for companies around the globe.** The underlying causes of insecurity, be they social unrest, geopolitical violence or societal risks, manifest themselves in many ways—physical threats and cyber threats among them. These threats, and the efficacy of the political and business organisations tasked with addressing them, have the potential to affect and curtail business decisions.
- **The causes of security risks, while far-reaching and diverse, are amenable to collective action.** In the survey, poverty, income inequality and resource scarcity topped the list of external threats corporations cite as risks to their physical and cyber security. Many of these lie beyond the scope of any single company or collection of companies to influence. However, many executives believe that the business community is beginning to collectively address a number of criminal exploits driven by the motivations, particularly those related to cyber insecurity, and that more such action is feasible and desirable.

- **Collective action on root causes of insecurity is likely to become more prevalent after internal security efforts reach a level of maturity.** Organisations, particularly smaller ones, often struggle to develop and fund credible security programmes. And many companies, regardless of size, have not embraced collective efforts to address root causes because they look to government entities to make changes. However, larger and more sophisticated organisations are embracing greater cooperation and coordination to address deeply rooted threats, particularly around cyber security issues.
- **Root causes of insecurity are increasingly on the radar.** Survey respondents agree that corporate boards need a better understanding of the underlying causes of insecurity and that cyber threats receive insufficient political attention. There is an acknowledged need to better understand security threats among corporate leadership, and it's worth noting that many interviewees cite progress on this front.
- **Physical and cyber security issues are converging.** The underlying drivers of insecurity create both physical and cyber risk. And, indeed, the two kinds of risk are converging. On the one hand, the best technical IT security solutions will be weakened if personnel access is poorly controlled; on the other, improved physical security relies more and more on digital systems. Corporate leaders must recognise this convergence; management structures and mitigation efforts must also take this convergence into account.
- **Obstacles to confronting the causes of insecurity are many.** Business leaders are trying to assess security risks honestly and comprehensively but the survey finds little consensus about the chief obstacles that prevent or constrain companies from taking a

more active role in addressing underlying causes of risk. The most frequently cited reason is that no agreement exists within the organisation on how best to address such issues. Additionally, many companies feel their interference would be frowned upon by political authorities.

- **Executives show confidence in political and organisational authorities' ability to mitigate the causes of insecurity.** In an uplifting show of faith, two-thirds of executive survey respondents say the business community and political authorities in their home countries are well-prepared to address systematically the causes of insecurity.
- **While businesses and political authorities put those efforts in place there are some immediate avenues companies can take to better address the threats they face.**
  - *Education.* There is growing recognition of the need for education efforts—both internally, among employees whose buy-in is important to make a security programme effective, and externally, so the public becomes savvier about threats. This is particularly true of cyber security.
  - *Cooperation and joint efforts.* Interviewees say that in pursuit of greater cyber security, cooperation among public organisations and private authorities has greatly increased in just the last few years. This shift, along with the development of alliances and forums for information sharing, indicates that threat information and response tools are being deployed more effectively. In some instances, cooperation now occurs almost in real time in response to attacks or incidents. Organised action in which multiple players come together with a plan to address points of vulnerability are also getting increased attention from corporate leaders and cyber specialists. ■

# Assessing the security challenge

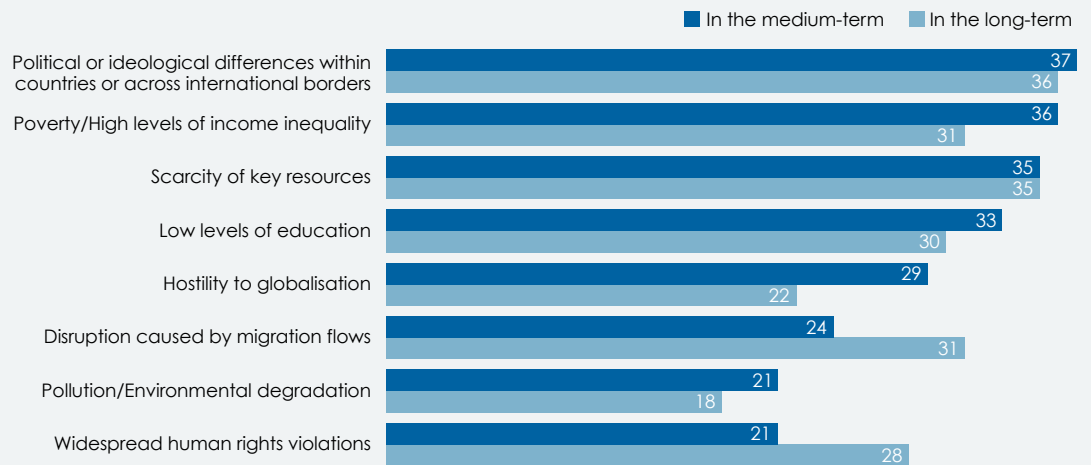
Shaping a security strategy that encompasses motivators of criminal activity.

Addressing systemic global concerns, such as income inequality and hostility to globalisation, are naturally considered beyond the scope of corporate security efforts. However in the EIU executive survey,

global leaders say these security concerns both physical and cyber in the medium and long term are impacting—even compromising—business decisions and security activities.

## Worldwide, what do you think will be the biggest root causes of insecurity in the next five years?

(% respondents, top eight responses)



Source: Economist Intelligence Unit survey, 2017.

Executives believe hostility to globalisation will be a lesser cause of insecurity in the long-term.

Corporate executives and consultants interviewed for this research say that even a well-conceived, properly executed security program can't eliminate or protect against all threats. "There's no amount of money that a company can spend for a guarantee that

they're going to be safe," says Arvind Parthasarathi, co-founder and CEO of Cyence, a startup that develops economic models of cyber risks for the insurance industry. "You can't dial it down to zero."

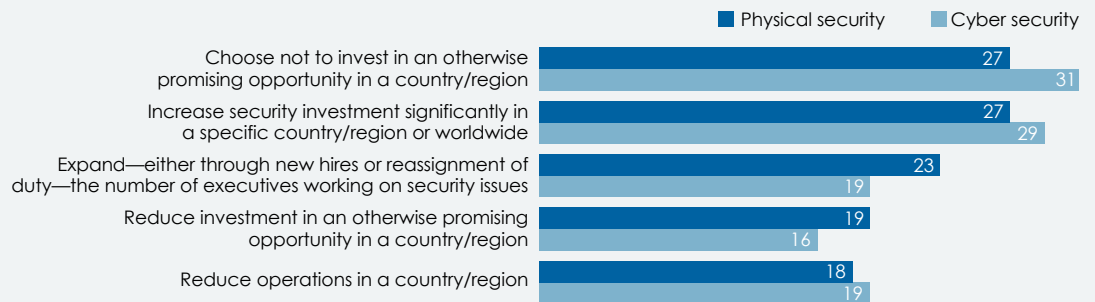
Strong security therefore can become a

competitive edge, or open up business opportunities that would otherwise be too risky. More than one-quarter of survey respondents say they had decided to not invest in otherwise promising opportunities in

certain locations due to physical or cyber security concerns. For nearly one-third of respondents, physical or cyber security risks have resulted in increased security investments. ■

**Have physical or cyber security concerns caused your company to do any of the following in the past three years?**

(% respondents, top five responses)



Source: Economist Intelligence Unit survey, 2017.

Executives say security-concerns have caused their company to change investment and operational decisions.



# Converging physical and cyber security risks

When asked about the how substantial a variety of types of threats are to their operations, more than half of respondents (57%) say risks to cyber security that could disrupt their business are an above or well above average concern. Corrupt officials came in a near second at 51%. And 49% say risks to the security of physical assets are an above-average concern, along with risks to sensitive or commercially valuable data (48).

Regardless of how threats manifest, the increasing convergence of physical and cyber security risks is notable. Organisations will reap advantages from managing them in a cohesive way. "I don't make a distinction between physical security or cyber security or information security," says Troels Oerting, who joined Barclays Group Plc as chief information security officer (CISO) at the start of 2015 and recently added the chief security officer (CSO) title.

Technology has undoubtedly become an integral part of the physical security of factories and offices, notably through badge readers, networked cameras, and facility automation. "All of that is ripe for disruption, where a cyber attacker can help facilitate or ease the physical penetration of an area," says Matt Devost, the co-founder of FusionX (now part of Accenture Security), a firm that tests a client's security defences with a so-called "red team" engagement that simulates a real breach. In turn, a physical security lapse can be one of the biggest threats to IT security. "Once you're on the premises, you have access to network

jacks and USB ports and all sorts of things from a cyber-attack perspective that become obviously very useful to you," says Mr Devost. Accenture acquired FusionX in 2015, and Mr Devost now oversees the consulting firm's cyber defence practice, which includes FusionX.

Robert Coles, CISO at GSK, the British pharmaceuticals group, points out how computerised building controls create at least the possibility that a cyber criminal could pose a serious risk to the physical safety of offices, factories and personnel. "If you can hack building management systems, you can stop people from leaving buildings, suppress fire alarms, that kind of thing," Dr Coles says.

Mr Oerting agrees that physical security breaches are a disaster for cyber security. If a motivated actor wants your money or information or intellectual property, they are going to go after it from the outside if they must, he says, but from the inside if they can. "You typically have much easier access to your network from the inside than you have from the outside."

In response to the convergence of cyber and physical risk, Mr Oerting says many innovative efforts in security also blur the line between cyber and physical measures. For example, surveillance of IT systems might include the tracking of data on the locations where employees typically log into their computers, such that, if there's a sudden change in that behaviour, the anomaly might be flagged as a security concern. ■

# Identifying the hurdles to corporate involvement

If security is a high and growing priority for organisations and executives know that many risks have societal causes, why are so few active in tackling the underlying motivations? When asked to identify “the leading barriers to adopting a more active role in helping to address root causes of insecurity”, respondents give a variety of answers.

The most common reason, cited by 30%, is the lack of agreement on how best to address these issues. And 27% say such activities would be “contrary to the corporate culture”. Another common answer, cited by 26% of respondents, is that the company “does not have the resources” to deal with the underlying security issues in more than a marginal way; 24% say the company “does not have the skills nor the knowledge” to do so. A lack of agreement and divergent

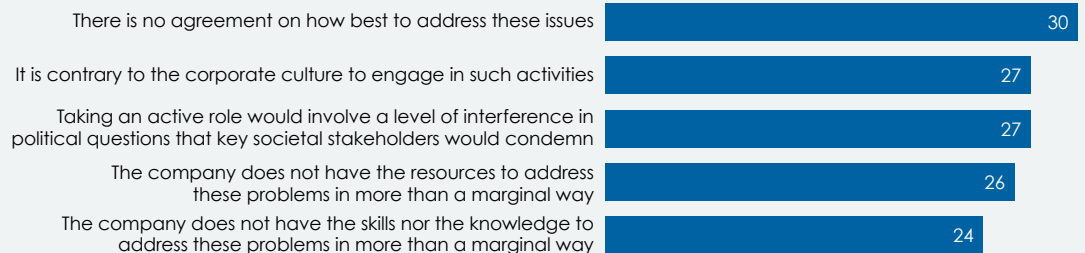
corporate culture suggest that companies need to hold discussion about these issues. Such steps could be followed by the allocation of more resources and development of relevant talent.

More problematic, perhaps, is the reasoning that, to address underlying causes of insecurity “would involve a level of interference in political questions that key societal stakeholders would condemn,” cited by 27%. For instance, the ethnic and religious tensions are arguably beyond the jurisdiction of corporate involvement. But income inequality and poor education are less so. For this to change, discussion of the role that businesses might play would have to go beyond corporate leadership and reach an audience among the general public.

Despite the barriers, corporate leaders

## What are the leading barriers to adopting a more active role in helping to address root causes of insecurity?

(% respondents, top 5 responses)



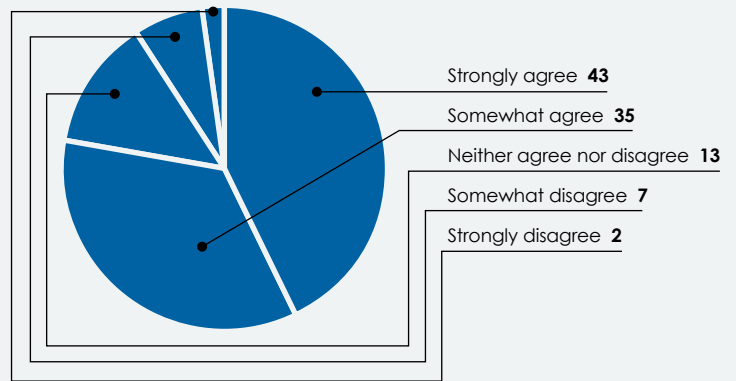
Source: Economist Intelligence Unit survey, 2017.

Executives say there is often no agreement on how to best address root causes of insecurity and that could not address the problems in more than a marginal way.

**Do you agree or disagree with the following statement:**

**The systemic risks of cyber attacks—their potential to shut down physical and financial infrastructure—gets insufficient political attention.**

(% respondents)



Source: Economist Intelligence Unit survey, 2017.

Executives believe the systemic risks of cyber attacks, and the potential impact on businesses, receive insufficient political attention.

express confidence that both political authorities and the business community are well-prepared to systemically address the motivations of insecurity. Nearly Three-quarters (71%) of the business community say the political authorities in their home countries are “very well-prepared” or “somewhat well-prepared” for that task. Curiously, companies that identify as top performers in their respective markets are even more optimistic about their environment than their less-prosperous counterparts.

This is not to suggest that companies believe that the security problems they face as a result of underlying issues are neatly on

course for correction. When asked about the degree of political attention given to the systemic risks of cyber-attacks (e.g. a potential shutdown of a company’s physical and financial infrastructure), 77% feel the political attention is insufficient.

It is often unclear who in government and law enforcement is responsible, says Mr Shiembob. Political leaders are in fact getting better at tackling cyber crime, but the issue is complicated by the fact that cyber crime crosses international borders, meaning the involvement of multiple governments will often be necessary. “It’s not an easy issue, but progress is definitely being made,” he says. ■

# Moving toward responsive leadership

Despite the hurdles to involvement, there is significant potential for corporate leaders to identify and address underlying security issues. And indeed the survey shows that attention to these insecurity risks is becoming a part of day-to-day C-suite and boardroom responsibilities, though that is not yet the standard.

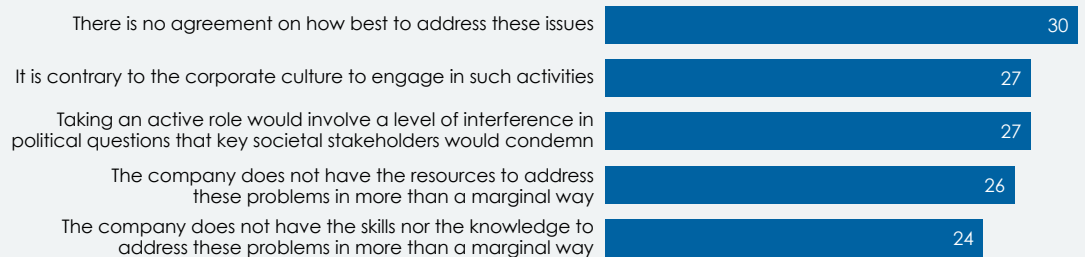
When asked who monitors and discusses today's security risks at their companies, 45% of survey respondents say the responsibility for monitoring "immediate risks to cyber security", rests with those who are directly in charge of cyber security. A combined 33% picked either C-suite or "both" (meaning C-suite and cyber teams). But looking ahead, when asked about responsibility for "emergent risks to cyber security," responsibility resting solely with the cyber team falls to 30%, with the portion of

respondents who picked C-suite or both jumping to 46%. In other words, C-suite involvement is seen as more relevant to the identification and assessment of longer-term, emerging cyber risks.

"This direct involvement of the C-suite is appropriate," says Cognizant's Mr Shiembob. He reports directly to the CEO and manages both cyber security and physical security. This inclusive approach to security and alignment to the C-suite helps to better integrate security into the corporate culture and provides proper emphasis. Such management alignment is far from universal in large corporate structures. Mr Shiembob says that at a recent conference for CISOs, a poll of the room showed that the "vast majority" still report to the chief information officer (CIO) rather than higher in the corporate structure.

## What are the leading barriers to adopting a more active role in helping to address root causes of insecurity?

(% respondents, top 5 responses)

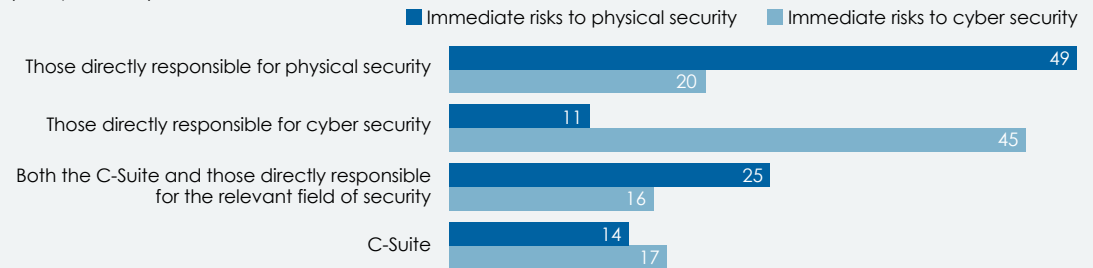


Source: Economist Intelligence Unit survey, 2017.

Executives say there is often no agreement on how to best address root causes of insecurity and that could not address the problems in more than a marginal way.

**Who is monitoring and discussing the following subjects at your company?**

(% respondents)



Source: Economist Intelligence Unit survey, 2017.

The security threats are climbing the agenda. Notably, the C-suite is increasingly involved in security discussions.

"This can be perceived as a conflict of interest," he says, since the CIO is likely to be focused primarily on the availability and utility of the IT infrastructure. Each company has different needs, but the trend is definitely towards combining security functions under a single leader with independent reporting to the C-suite or board.

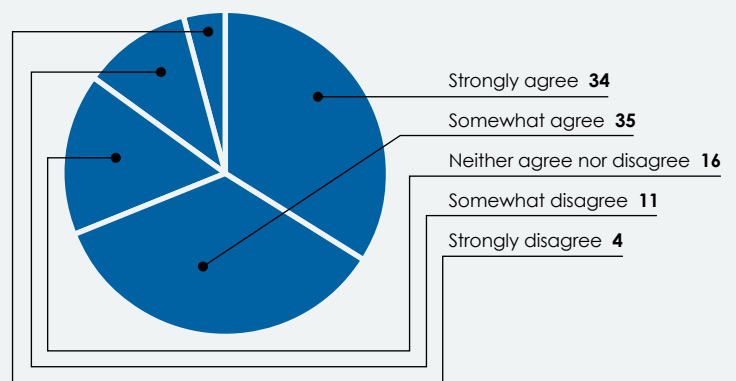
However, not all companies are in a position to incorporate such underlying security threats into their security strategy. Kevin Hyams, head of the Governance, Risk and Compliance group at Friedman LLP, explains that although motivations behind security risk are relevant to corporate decisions, companies may lack the

management structure capable of designing the proper responsive and proactive security policies to address them. "Particularly within smaller companies, this is just not on the agenda." He cites the example of a small US healthcare organisation that contracted with his firm: "They're just struggling to put in at least enough defences that they can justify to their donors, to their board, and to executive management, that they're paying due diligence to this particular exposure, consistent with their risk profile and resources." Insofar as they are worried about just getting their own house in order, they do not have the luxury of looking at the wider societal root causes, Mr Hyams adds. ■

**Do you agree or disagree with the following statement:**

**My company gives cyber-risk insecurity sufficient priority in its overall security programme given the risks they pose.**

(% respondents)



Source: Economist Intelligence Unit survey, 2017.

# Approaching insecurity battlegrounds: identifying vulnerable areas

Though companies do not have an appetite or understanding of how they can fully address the global insecurities underlying the threats they face, they are certainly looking beyond their immediate horizons to reduce their exposure to insecurity.

The following are examples of companies broadening their horizons by developing solutions to underlying problems rather than directly tackling the root cause. These are battlegrounds where the actions of destruction taken by criminals take advantage of widespread and business-related insecurities and risk. But more importantly, these are areas that companies feel they can control and protect with all of their resources and knowledge.

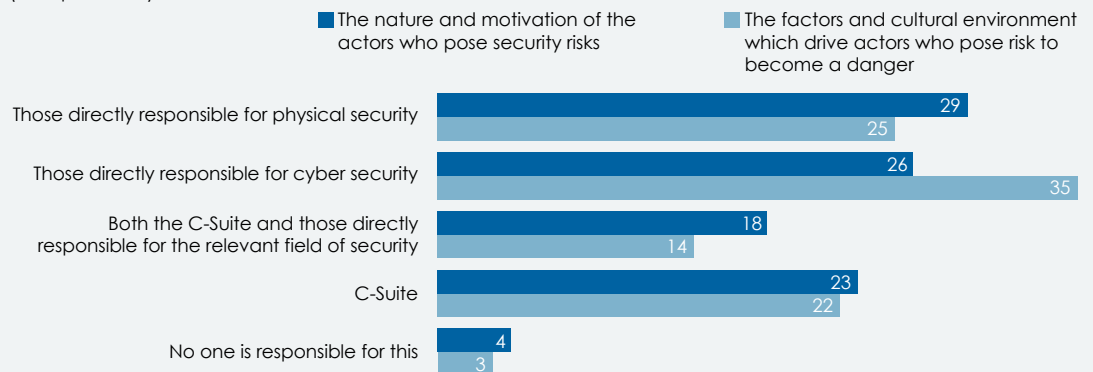
For example, security leaders often identify vulnerabilities in poorly defended or poorly managed infrastructures that can weaken over time. This is something that can be cited as a

battleground insofar as it allows cyber criminals to create the networks of malware-infected devices (botnets) and exploit the compromised servers. Accenture's Matt Devost refers to the persistence and sustainability of this "criminal infrastructure" as an area where "there's much more that can be done".

Seen from another point of view, poor security practices at some companies and among consumers—internet users—are ripe for solutions. By using weak or compromised credentials, they make hardware exploitation possible; in a similar vein, ignorance about phishing scams can defeat efforts to protect passwords. From yet another angle, hacker activity that's illegal but difficult to prosecute in foreign territory is a cause of cyber security threats. "To the extent that we can squeeze that safe-zone environment down and make the problem a little bit more manageable, I think it would be valuable," Mr Devost says. ■

## Who is monitoring and discussing the following subjects at your company?

(% respondents)



Source: Economist Intelligence Unit survey, 2017.

# Education matters

Executives and managers responsible for cyber risk management realise that education of their employees has to be a feature of any credible security plan.

Robert Anderson, head of the cyber security practice at Navigant Consulting Inc., says knowledge of cyber threats and what motivates bad actors is not yet sufficient within the leadership of most companies. "Some boards are starting to get smarter on it, but the majority don't really take the time."

Indeed, survey respondents touch on the role for education up and down the ranks of their organisations, identifying a need for greater knowledge of root causes of insecurity among board members. Fully 70% say they strongly agree or somewhat agree with the statement, "My company's board needs a better informed understanding of the underlying causes of insecurity", versus just 9% who say they strongly or somewhat disagree.

Friedman's Kevin Hyams underscores the importance of internal education efforts. He notes that an employee, even with the best of intentions, may take a laptop home for the

weekend and lose it; or he or she might find a thumb drive that's been planted by a bad actor and contains malware, pick it up and plug it into a workplace computer. There are many other ways poorly informed personnel can derail a security plan. "The weakest link is the malicious or careless employee," Mr Hyams says. In a very real sense, lack of education is an addressable cause of cyber insecurity.

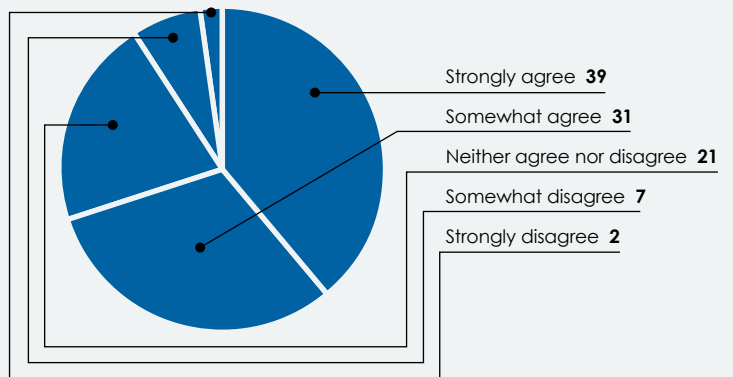
Indeed, interviewees consistently emphasise the need for security efforts to be integrated into the corporate culture if they are to be effective. Henry Shiembob, CSO at Cognizant, an IT consulting firm, says education and training are vital so that employees "understand the implications of what they're doing, not just to themselves, but to the company and to the people they work with."

Mohamed Alkady, founder and president of Hart Inc., a healthcare IT services start-up, endorses the idea that doing a better job of educating the public about cyber threats and safety could be an important way to address cyber threats.

**Do you agree or disagree with the following statement:**

**My company's board needs a better informed understanding of the underlying causes of insecurity in the country where I am based.**

(% respondents)



Source: Economist Intelligence Unit survey, 2017.

Mr Alkady notes that educating employees about better IT security in their workplaces is a potential starting point, as this is a rich environment where a lot of knowledge can be spread. The benefit could potentially go well beyond an employer's discrete security purposes. But it needs to be deliberate. As things stand now, many workers embrace best practices at work and then go to a bar or gym and leave their phones unlocked, use the same weak password for every purpose and so on.

A natural opportunity arises for public education, Mr Alkady suggests, when customers are interacting with sensitive data, such as their banking, brokerage or payment-related apps and websites. Banks commonly require passwords of a certain strength, but they do a poor job of both explaining why the password should be unique or of engaging with the customer on salient security points. "Imagine how much more impactful that would be if your bank told you: Hey, based on your password length it would take a hacker

one year to crack your password," Mr Alkady says. "Versus, if you add a letter, then it would take a hundred years to crack your password." That's technology that banks could implement today, he says, and it's an example of the kind of creativity that might provide a real boost to public education efforts.

Cognizant's Mr Shiembob says he spends a lot of time within his company raising awareness of cyber security and encouraging employees to pay attention to how their actions can affect the overall company, their coworkers and their job. Government could play a role in educating the broader public about these issues—the need for strong passwords, for example, or how to avoid phishing scams. Just as there are public service announcements about emergency preparedness or the dangers of smoking, there could, perhaps, be a state-run campaign of cyber safety education, he suggests. ■



# Cooperation and collective action

Not long ago, and in some places still, companies viewed knowledge of cyber threats and assessments of IT infrastructure defences as something to be held close, something that might even provide a competitive advantage. Graeme Newman, chief innovation officer at CFC Underwriting Ltd., a cyber insurance specialist firm, says that view has largely reversed within up-to-date businesses, with the growing realisation that every organisation is more secure when all are more secure—and that sharing threat information helps boost security.

"I firmly believe that making the internet safer for everybody is not a competitive differentiator," says Barclays' Mr Oerting, who is serving this year as chairman of the Global Cyber Alliance, a partnership with businesses formed by law enforcement agencies in New York and London. "I think we should share more than we do." In that pursuit, Barclays has helped spearhead the Cyber Defence Alliance in the UK, which includes a half dozen banks and law enforcement.

"I believe that if I'm hacked on a Monday, my colleague bank will be hacked on a Tuesday," Mr Oerting says. By sharing information about the first hack, the second one might be prevented. "That is the greater good." It's not all that different from calling the police if you were to see someone with a shotgun heading into a competitor's bank branch, he says.

This shift towards greater cooperation has occurred along with the maturation of companies' cyber security strategies, Mr Newman says, adding that he believes US organisations generally are more mature on cyber issues than their UK counterparts. One place where the change in attitude and

improvement in information-sharing can be seen is in the proliferation of ISACs (Information Sharing and Analysis Centres) and in the growth of their memberships. These centres are organised by industry and now cover healthcare, electricity, automotive and many other sectors. The Financial Services ISAC has been particularly successful, Mr Newman says.

Law enforcement has made efforts to promote information sharing and cooperation in the interest of greater cyber security for many years. In the US, the Federal Bureau of Investigation runs a programme called InfraGard, a public-private partnership with chapters in the agency's offices across the US and participation by 400 companies from the Fortune 500. InfraGard is meant to facilitate sharing of cyber threat information to help protect infrastructure from attack. Similar efforts can be found that involve law enforcement agencies in Europe and elsewhere.

"There are so many things that the government side does that people don't know about, and the intelligence that they gather and can share with the private sector is very important," says Mr Anderson, who was the third-highest official in the FBI before he retired and joined Navigant a year ago. InfraGard and related programmes help manage security clearances that might otherwise inhibit information-sharing, he says.

Some forums for cyber defence collaboration are less effective than they might be, because membership is limited to companies in just one country. Kelly Bissell, managing director at Accenture and head of the company's global security practice, highlights the need for cooperation that has the same global span as the cyber security

threat. "Attackers aren't bound by borders or country," he says, adding that the key point in fostering better cooperation on cyber security is this: "How do you share the data that matters, wherever it comes from?"

Notably, it's not just the sharing of threat information to anticipate and to prevent cyber attacks that has become more common. Real-time cooperation in the midst of an incident is more likely than it has ever been.

Consider just one example, the 2016 distributed denial of service attack on Dyn Inc., a provider of domain name system services, which rendered some of the biggest sites on the internet unreachable by customers in the eastern US for several hours on October 21. One of the underlying causes in this instance was a botnet made up of devices infected by malware, but cooperative efforts helped to blunt the attack and diminish its effect.

This event unfolded with unprecedented volume, as spurious requests came from tens

of millions of IP addresses. The attackers made use of internet-connected devices such as digital cameras and video recorders that were infected with Mirai malware, demonstrating an emerging threat from the Internet of Things (IoT). While this attack was fought off by the defensive tools that Dyn deployed, it also served to highlight how collective action might be useful to address causes of insecurity—internet-connected devices with weak security features.

In a company statement released the day after the attack, Dyn chief strategy officer Kyle York explicitly thanked "our partners in the technology community, from the operations teams of the world's top internet companies, to law enforcement and the standards community, to our competition and vendors", for their help in understanding and addressing the attack.

"What was interesting is how much the internet community banded together to help them," Mr Alkady says. "That's how you're actually going to get ahead of these things." ■

## Joint efforts in early stages

In addition to the informal cooperation among those managing cyber threats, more serious examination is being given to formal, coordinated efforts that deliberately tackle difficult security issues. This could take the form of new standards, or a well-developed leadership consensus that would affect behaviours.

For example, there is ongoing discussion and debate about how joint efforts might force or persuade device manufacturers to add more robust security features to everything they sell. The Dyn episode highlighted the ability of black hats to deploy internet-connected devices to create a denial of service attack of unprecedented scale. One of the obvious underlying issues that raised was the poor to nonexistent security features on some hardware, a particularly frightening state of affairs as the Internet of Things proliferates on the global network.

“Why on Earth are manufacturers allowed to ship connected devices which are wholly insecure?” Mr Newman asks. He argues that security standards should be put in place and makes an analogy to regulations and standards that ensure that electrical devices that get plugged into the wall will not suddenly burst into flames.

Makers of internet-connected consumer devices face competitive pressure to keep prices low, making it likely they will reject the extra expense involved in making sure a device has appropriate security features. While some niche consumers do use security as a competitive differentiator, but this has not taken on main stream – possibly due to the additional cost being too great “There’s no

economic incentive for the manufacturer to make those devices secure,” says GSK’s Robert Coles. He sees a regulatory role here, with a need for governments to step in to foster some consumer cyber protection. “I don’t really see that happening anywhere at the moment.”

Indeed, while many interviewees express the view that there should probably be a role for governments to promote better cyber security, especially as IoT devices proliferate, none of them could cite a good model for that regulatory paradigm.

Mr Alkady argues that standards setting will always move too slowly to have any practical effect on cyber security. But even so, a culture of coordination among organisations to the benefit of strengthening the security of the internet in general, rather than a specific company’s defences, is a step in the right direction.

Coordination of this sort is still not common, but there are some examples. The Global Cyber Alliance, an information-sharing venue founded by law enforcement agencies, for example, has an initiative meant to make it easier to implement an existing email authentication protocol known as DMARC. The goal: encourage adoption of a measure that has the potential to diminish the incidence of phishing emails, which try to trick recipients into providing logins, passwords and other authentication credentials.

Mr Newman argues that phishing is the root cause of a large swathe of the most devastating attacks that occur on the internet today. DMARC authentication, if widely adopted, could potentially be a solution to this cyber threat, Mr Newman says. “I’m not

saying it's the total silver bullet", he says, but it could go a long way toward the goal of eliminating such frauds.

Internet security blogger Brian Krebs, who on his own site has faced attacks similar to what Dyn experienced, suggests in his

coverage that coordinated industry efforts are needed to set standards for connected devices. Such standards could prevent devices that cannot be defended, or devices that come out of the box with a default weak or non-existent password, from being sold. ■

## Conclusion and takeaways

Companies are increasingly aware that constantly fighting short-term battles is unlikely to significantly improve their security posture on an ongoing basis. But, as this report has shown, they are also reluctant or baffled by how to engage in addressing the big picture root causes of insecurity.

Instead, they are beginning to take the middle road, and extending the horizon of their security efforts beyond traditional “higher walls and stronger defenses” approaches. They are, for example, seeking to boost the level of security education among employees. And they are cooperating to fight back against cyber attacks and discussing avenues for in collective action against cyber criminals.

With those nascent initiatives as a starting point, here are a few takeaways for executives, board members and thought leaders. Even as the root causes that may motivate bad actors and create insecurity remain mostly out of reach, there are more immediate steps that are both possible and desirable and can help to tackle the security threats driven by underlying causes of insecurity in the world today.

- **Support cooperative forums.** Efforts in recent years to create structures that allow the sharing of threat intelligence and cyber security tools between companies and with law enforcement have been effective.

Corporate leaders should continue to lend support and resources to these groups.

- **Foster cooperation.** Encourage cyber security managers to share information about breaches and attacks outside their own enterprise—in real time when necessary to respond to an incident. Discourage outdated attitudes that might prevent such cooperation among organizations.
- **Step up education.** The need for better employee training has been embraced, but education of the public in cyber safety best practices has a long way to go.
- **Communicate with customers.** Companies that interact with internet users, especially in transactions that involve payments or sensitive data, have a special opportunity to educate those customers in better security practices—they should take advantage of those contacts.
- **Improve device security.** The need to get consumer device makers to implement more robust security protocols is urgent as the Internet of Things proliferates. Business and internet leaders should encourage discussion over how best to make that happen. ■

Whilst every effort has been taken to verify the accuracy of this information, neither The Economist Intelligence Unit Ltd. nor the sponsor of this report can accept any responsibility or liability for reliance by any person on this report or any of the information, opinions or conclusions set out in the report.

**London**

20 Cabot Square  
London  
E14 4QW  
United Kingdom  
Tel: (44.20) 7576 8000  
Fax: (44.20) 7576 8476  
E-mail: london@eiu.com

**New York**

750 Third Avenue  
5th Floor  
New York, NY 10017  
United States  
Tel: (1.212) 554 0600  
Fax: (1.212) 586 0248  
E-mail: newyork@eiu.com

**Hong Kong**

6001, Central Plaza  
18 Harbour Road  
Wanchai  
Hong Kong  
Tel: (852) 2585 3888  
Fax: (852) 2802 7638  
E-mail: hongkong@eiu.com

**Geneva**

Boulevard des  
Tranchées 16  
1206 Geneva  
Switzerland  
Tel: (41) 22 566 2470  
Fax: (41) 22 346 93 47  
E-mail: geneva@eiu.com