The Economist Intelligence Unit

An Economist Intelligence Unit briefing paper

SECURING THE DIGITAL CITY

Cyber-threats and responses

Sponsored by

NEC

Contents

About the report

Securing the digital city: Cyber-threats and responses is an Economist Intelligence Unit (EIU) report sponsored by NEC. The report analyses the results of a global survey of 200 executives with responsibility for supporting and managing critical infrastructure IT systems, as well as in-depth interviews with senior executives. In addition to the survey respondents, we would like to thank the following for their time and insights:

- Johan Rambi, Corporate privacy and security advisor, Alliander
- Hosuk Lee-Makiyama, Director, European Centre for International Political Economy
- Alan Seigrist, COO, G-Hub
- Atul Babu, Head of international solutions sales, PCCW
- Jin Kim, Global solutions architect, Schneider Electric
- Saibal Chowdhury, CEO, Urbanetic

The EIU bears sole responsibility for the content of this report, which was written by Ross O’Brien and edited by Chris Clague.

Introduction

While the IT systems of critical infrastructure providers[1] face the same level of risk from cyber-attacks as do other enterprises in the private and public sectors, a cyber-attack on critical infrastructure can have much broader and deeper consequences for society and the economy. This puts added pressure on IT decision makers and influences how they design, implement and maintain their cyber-defences. Accepting the fact that the threats are both constant and, in terms of the means and methods, constantly evolving, the key to successful mitigation is the development of a proactive strategy of monitoring and detection. This includes close collaboration with all stakeholders in critical infrastructure operations and the involvement of senior leadership in driving strategy.

These leaders must also embrace an open and collaborative management approach to keep pace with the fast-changing information technology environments in which they operate. Outsourced solution providers are increasingly relied upon by critical infrastructure managers to deliver cost-effective services and to help them stay on top of technology evolutions. Critical infrastructure providers also see the growing importance of independent, Internet-connected sensors and control devices (the 'Internet of Things') in helping to manage infrastructure more efficiently and generating more insight into the levels of service they provide. Similarly, the rise of smart cities compels critical infrastructure executives to work with other platforms and service providers to join up their information systems and increase the leverage they all receive from the data and insight they share.

This openness, at first, seems counter-intuitive to good cyber-security practices. Open systems and cross-sector integration increase the points at which a network is exposed to incursion, malware and other cyber-attacks. It also potentially weakens the management response to cyber-threats, as collaboration with multiple service providers can muddy a decision-makers' view of the chain of command. Yet IT openness will nevertheless be a positive development for their cyber-security efforts. IT solution out-sourcers are often more up-to-date in their cyber-security practices, and are experienced in managing them across infrastructure platforms. IoT sensors massively increase a critical infrastructure provider's ability to gather external data and monitor cyber-threats proactively. Smart cities allow cross-platform sharing of cyber-security best practices. Ultimately, critical infrastructure leadership that builds its IT capabilities with others increases, rather than diminishes, its cyber-security resilience.

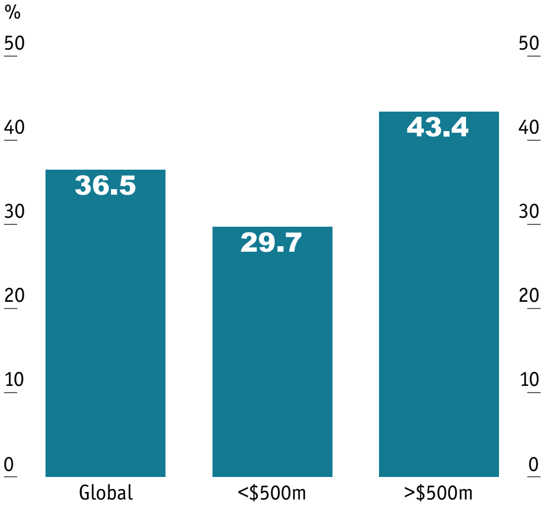
Bigger organisations, bigger headaches

Cyber-attacks are increasingly commonplace and the risk of them is rising, particularly among larger firms. Over one-third of survey respondents say their organisation has suffered a damaging cyber-attack in the last five years. There is also an apparent relationship between the size of firms and instances of attacks—less than 30% of respondents from smaller firms (those with less than US$500m in annual revenues) indicate that they have suffered an attack, while the response rate at larger firms

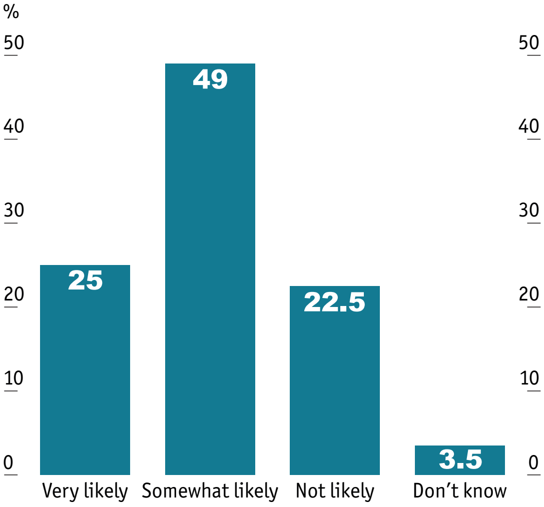
[1] Defined here as including transportation systems and ports, telecommunications networks, public safety operations, public utilities, and financial systems.

was 43.5%. This is perhaps unsurprising—as in most aspects of IT security, both the points of incursion and attractive opportunities for committing breaches increase with the size and scope of the network infrastructure deployed.

Respondents reporting a serious cyber-attack on their organisation in the last five years



Likelihood of serious cyber-attack in the next three years



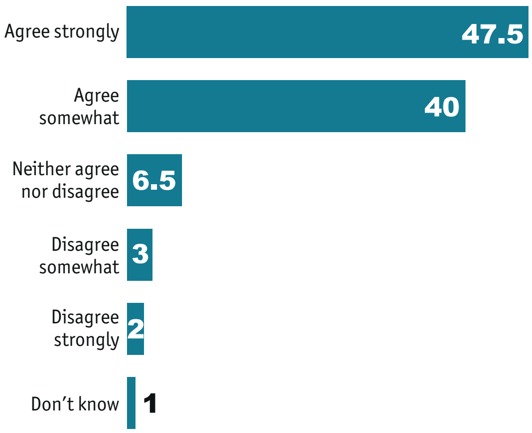
Respondents also expect the risks to increase. When asked the likelihood of a serious attack in the next three years, 74% of global respondents answered that it was either “very likely” (25%) or “somewhat likely” (49%).

Atul Babu, head of international solutions sales for Hong Kong telecoms carrier PCCW, agrees with this sentiment. “Information technology is constantly evolving, “ says Mr Babu. “Why would we not assume that cyber-attacks are also evolving and as quickly?” Security concerns are indeed a constant in IT management and as seemingly all commercial, economic, and civil transactions depend to varying degrees on the IT systems of critical infrastructure platforms, the potential repercussions of more frequent cyber-security incidents are thus severe.

Ready or not

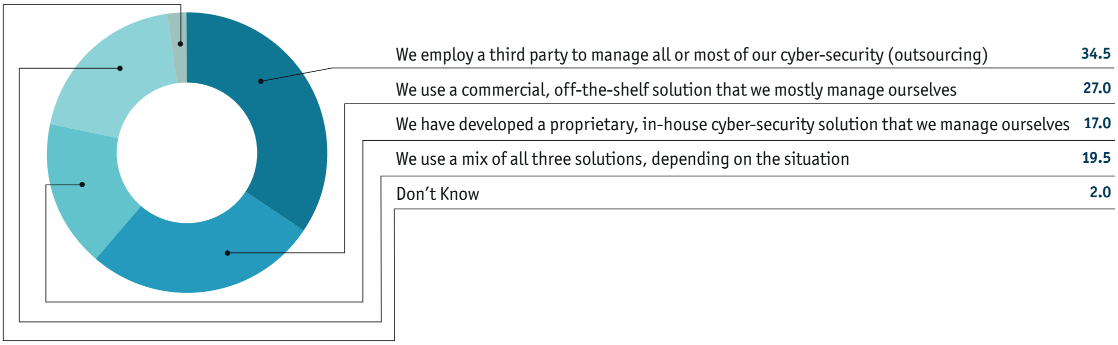
Critical infrastructure operators feel well prepared to deal with cyber-attacks, having moved from defence to offence and increased reliance on specialised external suppliers. Although a high percentage of respondents believe an attack is likely in the next three years, more than four-fifths also “agree strongly” or “agree somewhat” that their organisation has a clear chain of command for reporting and dealing with cyber-incursions.

My organisation has a clear chain of command for reporting and dealing with cyber-incursions
%



This is encouraging, if not somewhat surprising, given that a significant percentage of firms rely to varying degrees on outsourcing for their cyber-security solutions. Some 35% of respondents say they are primarily using third-party relationships to manage their cyber-security, a figure that is slightly higher (38%) among respondents from larger organisations. Another 20% say they use a mix of outsourcing, off-the-shelf and in-house solutions, while only 19% rely on their own internal resources. Outsourcing, once viewed with scepticism by security-minded technology buyers, seems to have gained acceptance as a key component of critical infrastructure providers' cyber-security efforts. It is also likely a response to a critically-needed resource amongst our respondents—cyber-security skills. A recent global study conducted by the Center for Strategic and International Studies (CSIS) found that 82% of organisations did not have sufficient skills to manage their cyber-security operations, particularly in the areas of intrusion detection and attack mitigation.[2]

What type of cyber-security solutions does your organisation currently have in place?
%



That chain of command may break down, however, when it comes to integrating cyber-security and physical security. The latter, for so long the only type of security that mattered to providers of critical infrastructure services, is changing in ways that mean those responsible for managing it must cooperate more closely with their counterparts responsible for the cyber side of the equation. That is not always easy, according to Johan Rambi, corporate privacy and security advisor at Alliander, a Dutch energy distributor, and not necessarily because of differences in approach or perspective. "The recognition of the need for cyber and physical security to cooperate and integrate is there," says Mr. Rambi, "but the challenge is to convince boards that the combined risk is equivalent to that of the

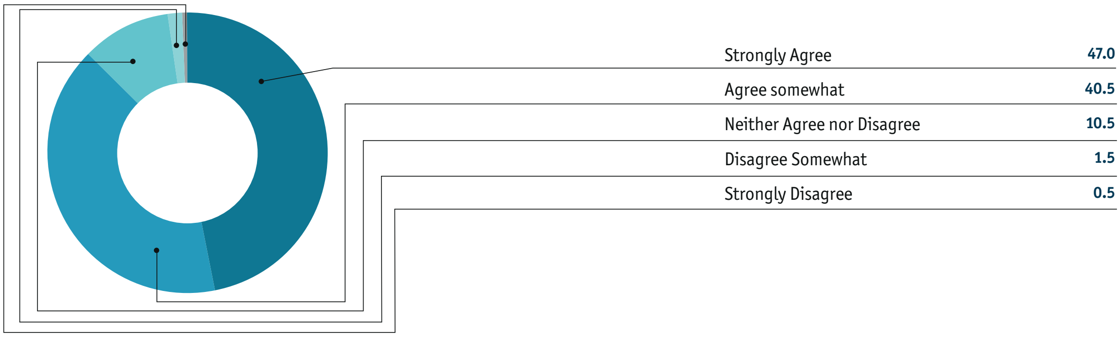
[2] http://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf

other types of risk they focus on, such as operational and financial risk. and that investing in uniting the two under one umbrella can solve problems and create new opportunities rather than just be a drain on resources."

The burden of intelligence

The Internet of Things (IoT), particularly in the smart city context, is viewed as both a vulnerability and an opportunity. In addition to the overwhelming majority of respondents who feel that a cyber-attack is at least somewhat likely in the near future, nearly 88% "agree strongly" or "agree somewhat" with the statement that their cities "must be more alert to critical infrastructure cyber-risks." This should not necessarily be interpreted as a widespread fear of impending doom. Rather, it is more likely an indication that technology decision-makers have accepted cyber-security issues, and their constant evolution, as a fact of life.

My city needs to be more alert to critical infrastructure cyber-risks
%



The rise of 'smart cities' is likely a probable source of their concern. While the term 'smart cities' is often used loosely to describe various municipal IT infrastructure projects, smart cities are most commonly thought of by critical infrastructure managers as cross-sector integration initiatives which link up the information technology platforms of private and public critical infrastructure providers, usually with a focus on healthcare, public safety and utilities. "Smart city architecture is built upon two fundamental principles," says Saibal Chowdhury, CEO of Urbanetic, a Singaporean firm which designs planning software for smart city projects. "One, data is transparent to as many participants as possible, and two, as many sources of intelligent, Internet-connected sensors and mobile devices as possible are connected to the integrated platform."

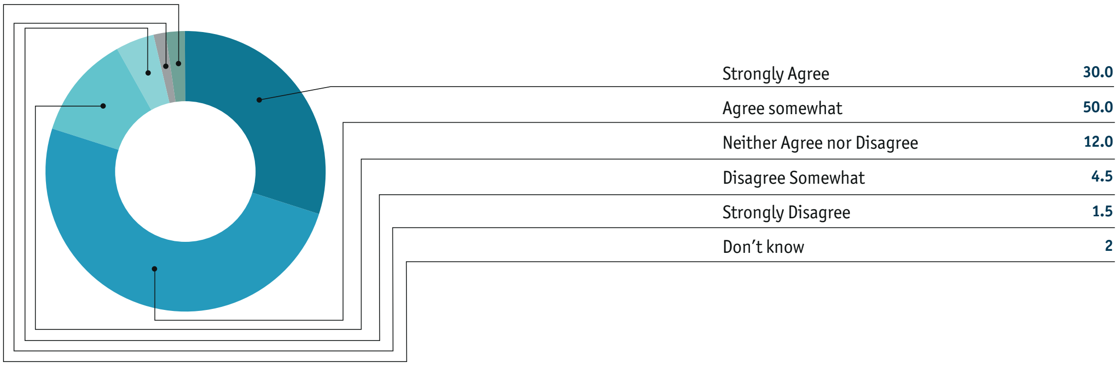
That these two principles are often in conflict further complicates cyber-security efforts. Data transparency, the first principle, is only facilitated by more cross-network integration, which, by its very nature, increases vulnerability. "Security guys only seek to lock things down," Mr Chowdhury says, "and the business and operations guys want to set all data free." He notes that, in order for cross-sector initiatives, like the creation of smart cities, to be successful, urban planners and municipal governments must establish a leadership hierarchy wherein a chief decision-maker co-ordinates and balances the needs of the various cyber-security architects and those responsible for data analytics and insights.

Increasing connections, increasing risk

The second of Mr Chowdhury's principles—that critical infrastructure IT systems must rely on an increasing number of Internet-connected sensors, appliances and other devices, otherwise known as the IoT—is also increasing cyber-security risks. It is shifting connectivity landscapes tremendously: analysts at Gartner estimate that 6.4bn 'things' (such as vehicles, sensors and appliances) will be connected to IT networks in 2016, and this will grow to 20.8bn by 2020.[3] The more potential points of entry to a network, and the more sources of valuable data, the more potential there is for attacks. Four-fifths of respondents believe that the IoT's rise will increase their organisation's vulnerability to cyber-attacks.

The proliferation of connected devices, the 'Internet of things' and 'Big data' will make my organisation more vulnerable to a serious cyber-attack

%



At the same time, the IoT is seen as an inevitable—and essential—part of building critical infrastructure. Data-gathering sensors that monitor traffic flows and energy consumption help make city streets safer and facilities more efficient, among other benefits. Gathering and parsing insight from Internet-capable vehicles or consumer devices will assist critical infrastructure managers in planning and improving how ports, hospitals and public safety facilities function. "We know IoT is coming, and we know that its role in managing and improving critical infrastructure will be vast," says Alan Seigrist, COO of G-Hub, a Hong Kong-based firm that deploys sensors for organisations in the US and Asia, "and we also know that it increases security risk. But if you don't deploy, you won't begin to understand IoT's potential benefits and that's a far bigger risk."

Interestingly, the rise of big data and the IoT is also seen as part of the security solution, at least in the long term, as the focus of cyber-security methodology shifts from building robust defenses (viewed as more and more difficult given the rapid pace of technology development) towards more proactive detection of the sources of threats and where they might occur. Deployment of a variety of sensors and analytic engines provides IT managers with the tools they need to build up those detection capabilities.

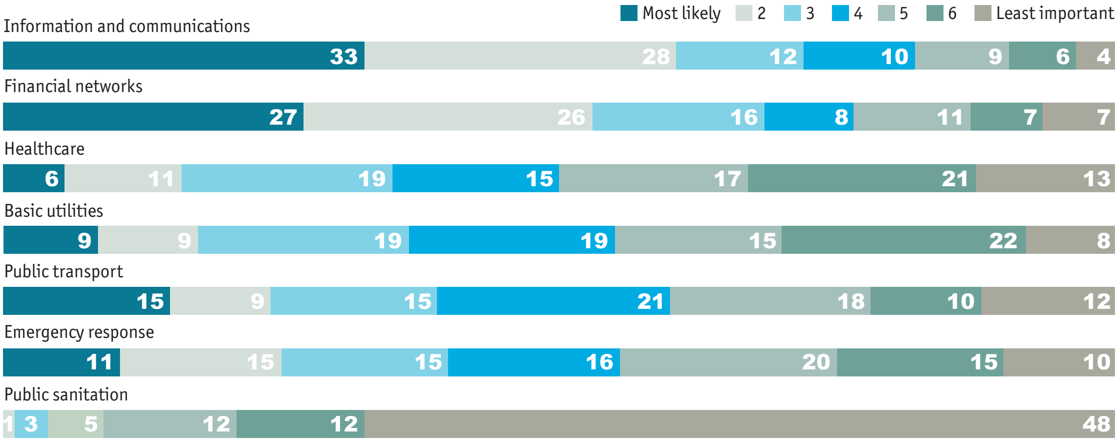
[3] http://www.gartner.com/newsroom/id/3165317

However, a shifting regulatory environment could present a roadblock to the use of various tools, says Hosuk Lee-Makiyama, director at the Brussels-based think tank, European Centre for International Political Economy. “The problem with critical infrastructure and cyber-security is that it’s becoming this huge grey area when it comes to regulation,” says Mr Lee-Makiyama. “Do the cloud services offered by a telecoms operator qualify as critical infrastructure? Is search critical infrastructure? There’s a tendency to expand the definition of critical infrastructure and that’s creating difficulties.”

Many vertical vulnerabilities, one horizontal

When asked which critical infrastructure networks are most vulnerable to cyber-attacks, roughly one-third of respondents indicated that telecom and Internet services providers are most at risk, followed by banking systems (chosen by 27%). Public safety, utilities and services are seen to be much less vulnerable. It is unsurprising that telecoms infrastructure is viewed as most likely to suffer a cyber-attack—it is, in the words of Mr Babu of PCCW “the horizontal platform that enables the technology platforms of all other critical infrastructure ‘verticals’.” Mr Babu points out that “The level of dependency that other critical infrastructure providers have on ITC connectivity places a unique burden on the telco provider”, and heightens their risk as a first point of incursion.

Which services are most likely to be the target of a cyber-attack?
%

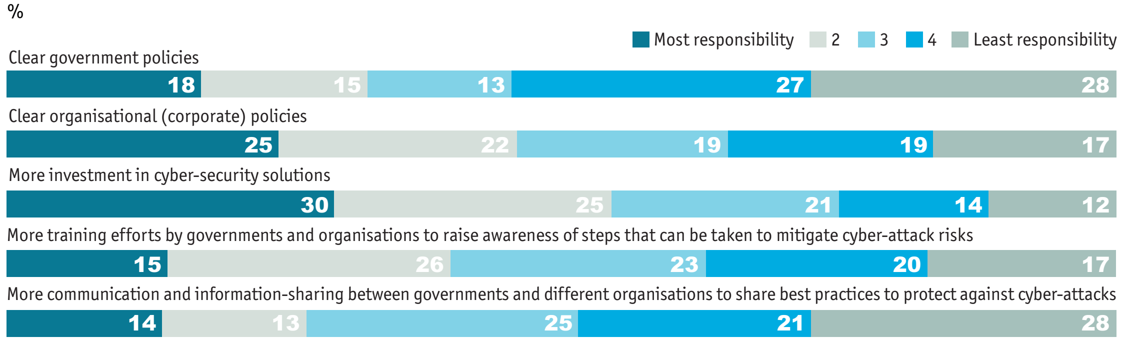


Similarly, it is not surprising that banking is viewed as the next most likely victim of cyber-attack, as “banking is a more ‘high value’ target,” says Mr Jin of Schneider Electric. Yet he also feels that the finance industry is more resilient than most other critical infrastructure providers. PCCW’s Mr Babu agrees, noting “banking is quite an advanced sector, in large part because it has no choice—it is an industry that is completely dependent on IT systems” to deliver its services. Banking’s cyber-security prowess also means that its threats are more contained. “There are still cyber-thefts, but usually at an individual bank level, involving a physical system incursion or ATM hack,” says Mr Jin. “Attacks are isolated and rarely at a global level.” This is because banking cyber-security teams have learned how to isolate and insulate their various system interfaces better, and are large adopters of analytics tools, which helps filter out weaknesses in systems.

It’s all important

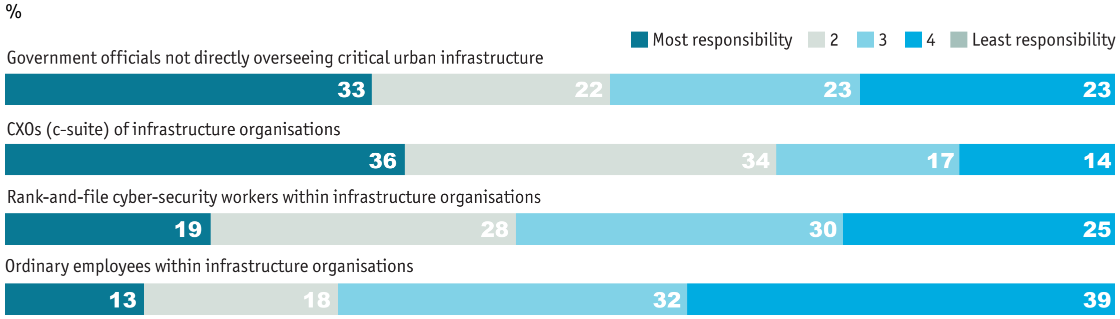
There is no single approach to cyber-security that will offer organisations protection. When asked to rank which tactics are most important in order to defend their organisations against future attacks, the responses were diffuse. “More investment in cyber-security solutions” was selected as the most important factor by 30% of respondents, followed by clearer organisational policies (25%), and better government policies (18%). This suggests that there is a general belief among decision-makers that a ‘portfolio response’ to cyber-security management is needed. In other words, all these tactics are important. The one exception, and a curious one, is the low priority assigned to cross-organisational communication. Critical infrastructure IT networks are, as discussed above, integrating with each other, and the wider IoT world around them: collaboration and coordination amongst all participants should actually be a greater priority, according to G-Hub’s Mr Seigrist.

Please rank the following as to how important they are in preventing future cyber-attacks on your organisation



Unsurprisingly, when asked where responsibility for the cyber-security of critical infrastructure should lie, the vast majority of respondents (66%) felt that it was with the offices of the most senior decision-makers in government or with the infrastructure providers themselves. Again, this is informed by the growing acceptance of cyber-attacks as a constant threat, and the fact that the ramifications of cyber-attacks are growing alongside the increasing inter-dependence of IT systems across multiple infrastructure platforms. Chief decision-makers in local government and civil bureaucracy, and the

Please rank the following by how much responsibility they should have over critical infrastructure cyber-security.



executives that oversee critical infrastructure, thus need to incorporate cyber-security strategies fully into their overall leadership, offering clear guidance to subordinates, outsourcers and collaborators.

Globally, respondents ranked infrastructure chief executives higher than mayors or city councils. Seventy percent of respondents felt chief executives held either the first or second-highest position of responsibility for cyber-security, while 52% felt government officials should bear primary or secondary responsibility. The bias towards organisational, rather than governmental, responsibility is likely a reflection of the perceived need for fast, responsive decision-making.

Conclusion

Cyber-attacks are a clear, constant threat to all organisations, and advances in information technology benefit perpetrators as much as the organisations who seek to thwart them. Critical infrastructure providers are not unique in their inherent vulnerability to attacks, but the fact that the services they provide underpin the very workings of civil society and the economy means the consequences of failing to defend against attacks are far greater. Moreover, the fact that critical infrastructure providers increasingly depend upon cross-platform integration with each other—and all intersect with the primary, 'horizontal' infrastructure of telecommunications and Internet networks—means that an attack on one can have magnifying effects on all of them.

Yet critical infrastructure managers are not resigned to constant, grinding cyber-warfare. In fact, the threats are serving as a catalyst for cyber-innovation—leaders are increasingly committed to integrating cyber-security-centric processes into their overall operational strategies, while also trying to build integrated smart systems that can learn from each other. This commitment is in large part an attempt to address the central challenge they face, says Mr Jin of Schneider Electric. "We are managing security in an IT environment defined by two diametrically opposing trends: we want our systems to be open so that we leverage the synergies and insight they provide, and yet network integration is a process directly opposed to security."

The 'insulation' of integrated systems will remain a challenge for critical infrastructure providers. It is further complicated by a lack of senior executives and government officials with the cross-sector leadership experience needed to implement this approach to security. But being open to external expertise and input from other critical infrastructure providers can help organisations to overcome these constraints by creating a proactive cyber-security that evolves and succeeds.

While every effort has been taken to verify the accuracy of this information, The Economist Intelligence Unit Ltd. cannot accept any responsibility or liability for reliance by any person on this report or any of the information, opinions or conclusions set out in this report.

The Economist Intelligence Unit

LONDON
20 Cabot Square
London
E14 4QW
United Kingdom
Tel: (44.20) 7576 8000
Fax: (44.20) 7576 8500
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 1181/2
E-mail: americas@eiu.com

HONG KONG
1301 Cityplaza Four
12 Taikoo Wan Road
Taikoo Shing
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
E-mail: asia@eiu.com

GENEVA
Rue de l'Athénée 32
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
E-mail: geneva@eiu.com