Security risks and responses in an evolving telecommunications industry

Telecommunications reach deep into the daily circumstances of individuals, businesses, and governments. Telecoms, in fact, touches nearly everything and everyone, and, along with energy, forms a foundation upon which all other critical infrastructure operates.

Therein lies the appeal to cyber adversaries.

So, how is the industry combatting today's threats? Following are highlights of our findings among industry respondents who participated in The Global State of Information Security® Survey 2014*, a worldwide study conducted by PwC,* CIO *magazine, and* CSO *magazine.*

by Mark Lobel

Mark Lobel is a principal in the advisory practice of PwC US. For more information, contact Mark by phone at [1] 646 471 5731 or by email at mark.a.lobel@us.pwc.com.

For more information and to access the full results of *The Global State of Information Security Survey 2014,* visit www.pwc.com/giss2014.

CCTV security camera above King's Cross Square, London, UK.

A successful cyber attack on a telecommunications operator could disrupt service for thousands of phone customers, sever Internet service for millions of consumers, cripple businesses, and shut down government operations.

And there's reason to worry: Cyber attacks against critical infrastructure are soaring. For instance, in 2012, the US Computer Emergency Readiness Team (US-CERT), a division of the Department of Homeland Security, processed approximately 190,000 cyber incidents involving US government agencies, critical infrastructure, and the department's industry partners. This represents a 68% increase over 2011.[1]

Keeping abreast of rapidly evolving cyber threats – and the 'bad guys' who would perpetrate them – is a priority for telecommunications organisations, including Cablevision Systems Corporation, a multiple system operator (MSO) whose properties include cable TV, an Internet service provider, and a high-circulation daily newspaper.

"Like most MSOs, we are attuned to and follow the published reports denoting an increase in the detection of state-sponsored and cyber-terrorist activities, specifically as they relate to utilities and communication companies as targets," says Jennifer Love, senior vice president of security operations for Cablevision. "We use information from various sources, including the industry and government, to identify risks and guide decisions."

Telecoms operators are adept at protecting their networks. It's also true that cyber adversaries employ the telecom infrastructure as their primary transport for most attacks – and, as such, they rely upon a robust network. Consequently, adversaries who seek to attack telecoms are typically limited to anti-establishment hackers or nation-states seeking to use advanced persistent threats (APTs), according to Jamie Barnett, senior fellow of the Potomac Institute for Policy Studies and co-chair of the telecommunications group for Venable LLP, a law firm in Washington DC.

"That's not to say that telecom organisations are not under attack every day. They are," says Barnett, a retired US Navy admiral who also has served as chief of the Public Safety and Homeland Security Bureau of the Federal Communications Commission (FCC). "But as long as the bad guys and nation-states want the Internet to work as a means of carrying their malware, attacks, and criminal endeavors, the telecoms can handle the attacks. But they are still vulnerable."

Today telecom organisations, particularly large global operators, are recasting themselves as technology companies. They are, for instance, creating mobile applications for use of VoIP calls and storing data on cloud services. Combined, mobility and cloud computing create new frontiers of risks for operators that will expose them to many of the same security risks that tech companies must dodge.

One mounting technology concern among operators is Internet route hijacking, also known as IP hijacking, an exploit in which adversaries corrupt

Today's cyber adversaries are constantly sharpening and evolving their capabilities to exploit new vulnerabilities. Addressing these threats will require that telecoms operators approach activities and investments with comprehensive, up-to-the-minute knowledge about information assets, ecosystem threats, and vulnerabilities.

Internet routing tables to 'hijack' packets of data. Possible solutions include implementation of secure Border Gateway Protocol (BGP), a technology that can be used globally. Trouble is, while BGP has been around for a while, secure BGP standards haven't been consistently adopted, and that's not likely to happen without government incentives such as tax breaks for public-sector operators.

Another technology challenge can be found in the telecommunications supply chain that comprises control layer equipment such as computer hardware, software, and middleware. The fact that much of this equipment is manufactured in different parts of the world has made it a 'third rail' that's rarely discussed, according to Barnett.

"The control layer for telecoms links back to the manufacturer for software updates and patches. The location of the manufacturer may raise some security questions for certain operators," Barnett says. "From a national security standpoint, you could shut down an entire network from the telecommunications control layer."

A new survey shows gaps in security practices

Today's cyber adversaries are constantly sharpening and evolving their capabilities to exploit new vulnerabilities. Addressing these threats will require that telecoms operators approach activities and investments with comprehensive, up-to-the-minute knowledge about information assets, ecosystem threats, and vulnerabilities.

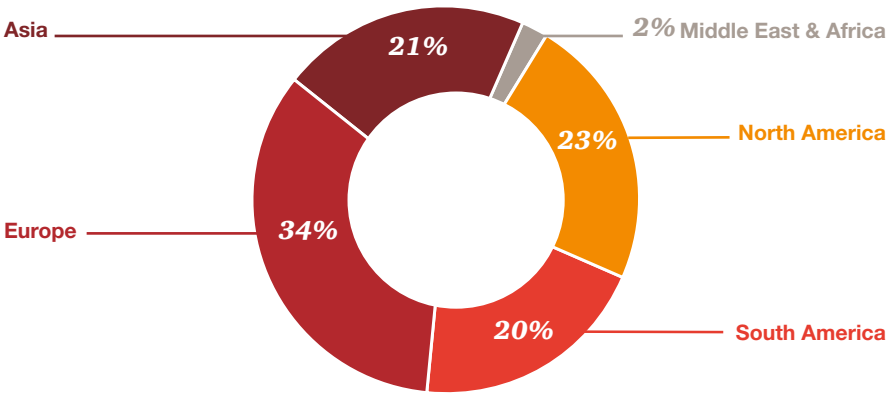
Operators have made longstanding contributions to critical infrastructure and technology innovation, and our research indicates that they are prepared for some, but not all, of today's information security challenges. *The Global State of Information Security® Survey 2014*, a worldwide study conducted by PwC, *CIO* magazine, and *CSO* magazine, polled 456 telecommunications executives to measure and interpret how they combat today's cyber threats.

Some of the results were surprising. For instance, while the number of security attacks against critical infrastructure has been rising, the annual study found that telecoms executives detected 17% fewer security incidents over the past 12 months, compared with 2012. Respondents also reported a decrease in the financial costs attributed to security incidents.

In comparison, security incidents have increased by most measures, with overall survey respondents from all industries reporting a 25% jump in detected incidents. The fact that telecoms organisations are not reporting more incidents suggests, in part, that old security models in use may be ineffective against today's sophisticated attackers.

Parsing the survey data a bit more uncovers some worrisome trends. For instance, the number of respondents who don't know the frequency of security incidents continues to climb year over year – it's now at 19%, up from 14% last year and 8% in 2011 – which serves to contradict the notion that organisations are becoming better at detecting and responding to intrusions.

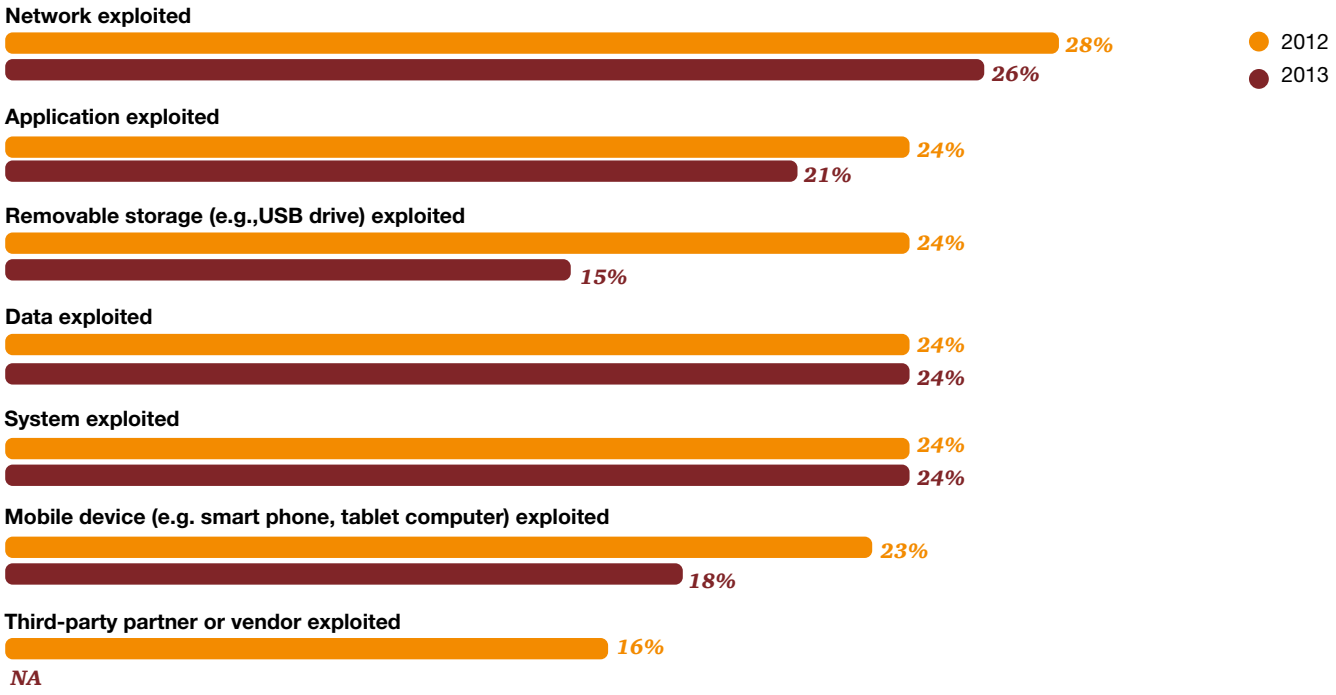
Figure 1: Telecom respondents by region



Source: *The Global State of Information Security Survey 2014.*

Figure 2: Type of security incident

Question 19: "What types of security incident(s) occurred?" (Not all factors shown.)



Source: *The Global State of Information Security Survey 2014.*

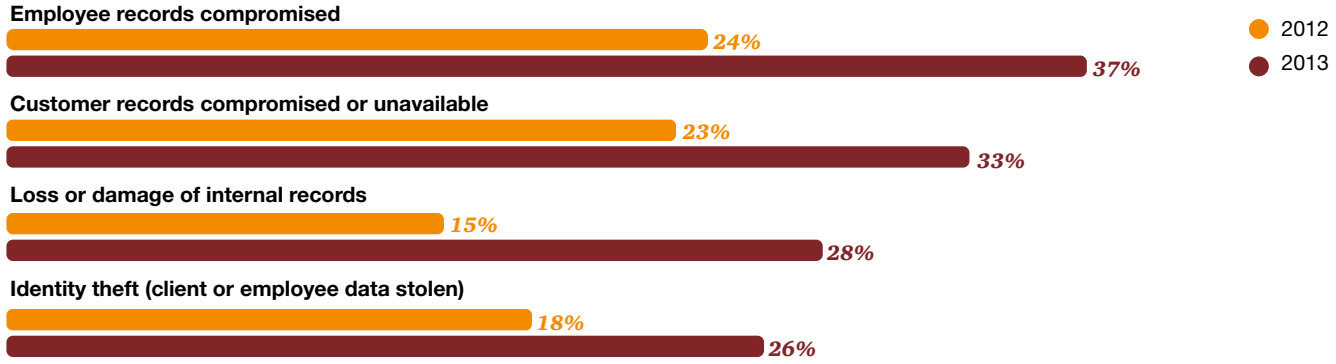
Another factor to consider is downtime of networks, applications, and services, which jumped this year to an average of 21 hours, up from 15 hours in 2012. Exploitation of networks was the most commonly cited impact of security incidents, followed by compromise of data (see Figure 2). When networks are down, so are operations and brand reputation among customers and consumers.

What's more, breach of employee and customer information also increased substantially over last year, potentially jeopardising an organisation's most valuable relationships (see Figure 3). Telecoms reported that compromise of employee records increased 54% over 2012, and breach of customer records jumped 44%. Safeguarding customer information is critical because, as one telecom executive says, "If you don't have customers you don't have to worry about new devices or services."

And among telecoms organisations that experienced a security incident in the past 12 months, 20% reported financial

Figure 3: Impact of security incidents

Question 22: "How was your organisation impacted by the security incidents?"(Not all factors shown.)



Source: *The Global State of Information Security Survey 2014.*

losses due to breaches, a 15% increase from last year. Yet, the average costs of these financial losses were down 34% over the year before.

This paradoxical finding may be explained by the fact that many organisations don't perform a thorough appraisal of all factors that can contribute to financial losses. For example, only 39% of telecoms respondents considered damage to brand and reputation when estimating the full impact of a security breach, and only 25% considered loss of intellectual property. Just 41% factored in legal defense services, and investigations and forensics were included by just over one-third (34%) of respondents. The full picture, we believe, would result in a more significant tally of financial costs.

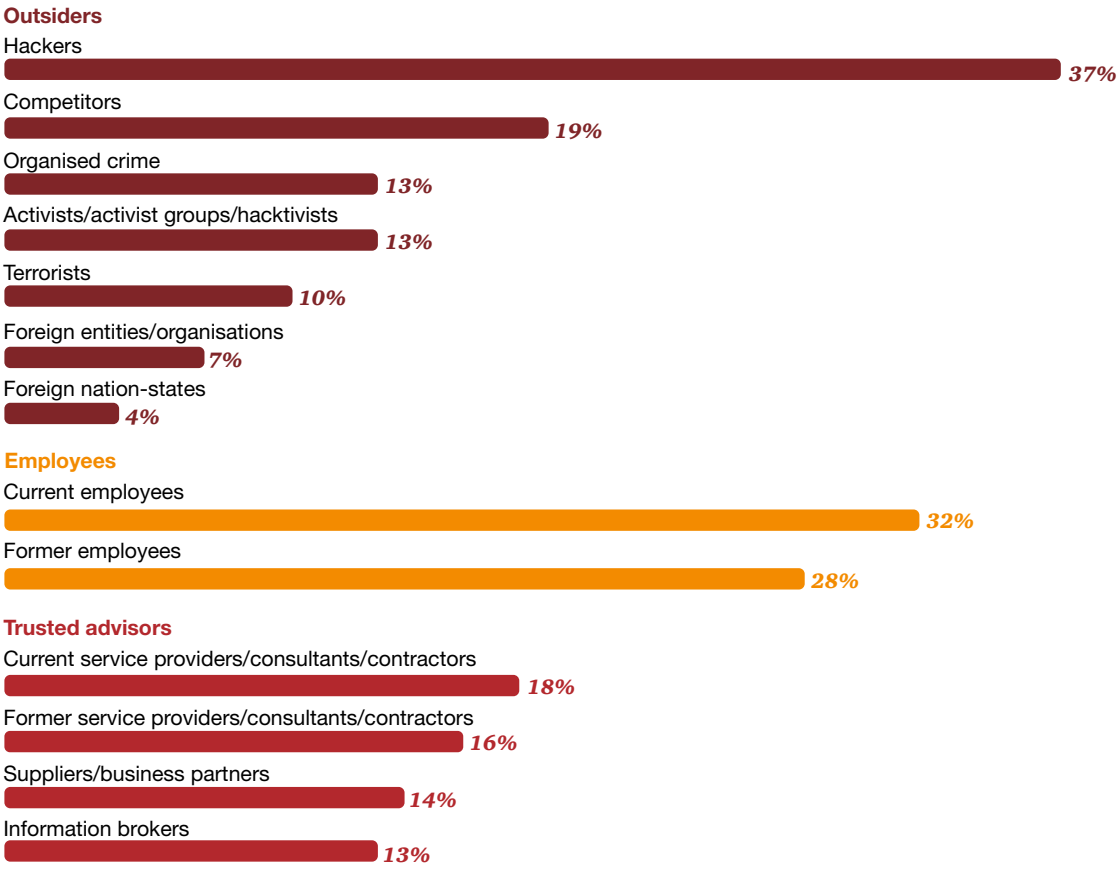
When asked to name the source of security incidents, the answers were not surprising: Hackers and employees remain the source of most incidents (see Figure 4).

Thirty-seven percent (37%) of respondents attribute incidents to hackers, a number that is both higher than other industries and a significant jump (23%) over telecoms responses last year. As a result, many operators are grappling to understand the might and motives of hacktivist groups like Anonymous, which have been responsible for many ideologically motivated attacks designed to bring about social change. Some operators are preparing their workforce to recognise and report the type of individual who may belong to such groups.

"I believe it's highly likely that some hacktivist groups may have resources already in place in many companies, as membership only requires a like-minded ideology," says Michael A. Mason, chief security officer for Verizon Communications. "I have challenged my team to ask what someone with an affinity for these groups might look like in this company."

After hackers, employees present the greatest threat to security. Almost one-third (32%) of operators cite current employees as the source of incidents and 28% lay the blame with former employees. Given the prevalence of employee risks – not a new threat vector – it's surprising that many organisations aren't prepared to handle common insider threats. A separate survey co-sponsored by PwC, the

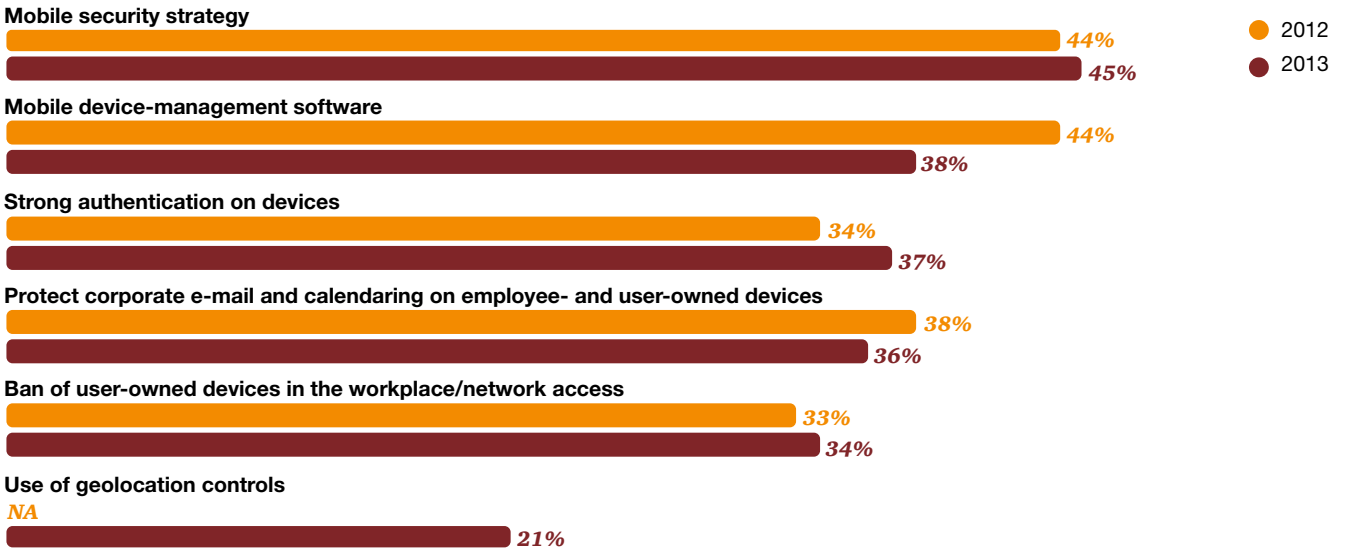
Figure 4: Estimated likely sources of security incidents



(Not all factors shown.)
Source: *The Global State of Information Security Survey 2014.*

Figure 5: Initiatives launched to address mobile security risks

Question 16: "What initiatives has your organisation launched to address mobile security risks?" (Not all factors shown.)



Source: *The Global State of Information Security Survey 2014.*

2013 US State of Cybercrime Survey, finds that one-third of US respondents across all industries don't have an incidence response plan for dealing with insider security incidents.[2] And among those that do have a response plan, only 18% of respondents describe the effort as extremely effective.

And what of highly publicised incidents such as attacks by foreign nation-states that employ advanced persistent threats (APTs) to invade a network for the long haul? Survey respondents said intrusions backed by foreign nation-states account for only 4% of detected incidents.

While that's hardly the preponderance of potential threats, keeping abreast of rapidly evolving cyber threats is, nonetheless, a priority for most operators. Employee awareness is a key component of fighting this type of attack, which often originates as well-researched phishing exploits that prompt specific users to click a link or document contained in an e-mail.

"One of the greatest challenges is the human element," says Barnett. "Telecoms can spend millions of dollars on cybersecurity, and yet when someone inside the company gets an e-mail and clicks on a picture of a cute kitty cat, that can infect the entire network. It's all about training employees."

Indeed, no security program will be effective without employee awareness, a security basic that is lacking at too many organisations. Fifty-nine percent (59%) of telecoms respondents said their company has an employee security awareness training program in place, up from last year. That's progress, but given the potential for damage that an uninformed or careless worker can unleash, all organisations should have training programs in place.

Mobility, the cloud, and intellectual property

Another front-burner issue for telecoms organisations is the proliferating risk of intrusions via mobile devices, whose ubiquity has compounded a number of security risks.

But if mobility represents a pressing security challenge for telecom firms, according to the survey, they have done little to deploy security measures. For instance, our data shows that only 45% of telecoms organisations have a mobile device security strategy in place, and fewer – 38% – employ mobile device management (MDM) software, which is essential to safeguarding a fleet of handhelds. Just 36% said they protect corporate e-mail and calendaring on employee- and user-owned devices (see Figure 5).

Here's another finding that caught our eye: A striking lack of security practices exists among telecoms organisations that have implemented customer-facing mobile applications. Only 34% of respondents said they have created secure mobile app development processes, and just 26% employ a unique set of network and firewall policies to protect data. Encryption of data is key in safeguarding information packets in the wild, but only 27% of telecoms respondents said they encrypt sensitive data in the mobile app and just 30% employ transport encryption.

As the use of mobile devices proliferates, so too does the use of cloud computing services. The cloud has been around for more than a decade, and today 50% of operators said they use some sort of cloud service – and of those, 57% said the technology has improved their information security. So it's a bit surprising to learn that

Telecoms organisations are boosting information security budgets significantly. This year, the survey found that security budgets average US$5.4 million, a gain of 35% over 2012.

many organisations haven't seriously addressed the security implications. For instance, while half of telecoms respondents report using cloud services, only 20% include provisions for cloud in their security policies.

It's imperative that operators implement policies that form the basics of cloud security, including data encryption, protection of business-critical data, ensuring that service providers adhere to security standards, and regulations regarding where data can be stored, among others. They should also require that third-party cloud providers agree to follow security practices.

Today organisations share increasingly more data with third parties, vendors, partners, and customers. One type of data that should not be freely allowed to leave the enterprise, however, is intellectual property (IP). Among operators, IP can include sensitive data such as long-term marketing plans, documents pertaining to mergers and acquisitions, financial data, and research and development documents. This type of information, which may be targeted for long-term economic gain, is becoming increasingly valuable.

As with any type of data, as the value of IP increases, so does its appeal to cyber criminals. Yet few operators have taken steps to ensure the privacy of these 'crown jewels.' In fact, the survey found that only 18% of telecoms respondents said they have procedures in place to protect IP, and just 17% said they classify the business value of data.

Another up-and-coming challenge for telecoms is guidance from the US Securities and Exchange Commission that calls on companies to include cybersecurity concerns in their regulatory findings. A survey by Intelligize found a 106% increase in references to cybersecurity concerns in SEC regulatory filings compared with the previous six-month period.[3] The firm, which specialises in SEC filings, says that 21% of these disclosures were from telecoms companies, and that while most companies broadly state the risk of being a victim of security incidents, many are now disclosing specific incidents of attacks.

How telecoms are improving cybersecurity

Telecoms businesses, as noted, tend to be comparatively adept at managing information security risks. And many are taking action to achieve an enhanced level of ongoing insight and intelligence into ecosystem vulnerabilities and dynamic threats.

Telecoms organisations are boosting information security budgets significantly. This year, the survey found that security budgets average US$5.4 million, a gain of 35% over 2012. And overall IT spending climbed to an average of US$162 million for 2013, an increase of 17% over last year. Despite this increase, however, information security budgets represent only 3.4% of the total IT spend this year, a relatively small investment that has remained constant in recent years, according to the survey.

Another measure of progress can be gleaned from how well executives believe their organisation's security program is aligned with business strategy and overall spending. By that count, optimism is robust: 72% of respondents said their security strategy is aligned to the specific needs of the business. This type of response level shows that, from top to bottom, security is becoming an elemental component of corporate culture and a top business imperative – not just an IT challenge. In other words, security is everybody's business.

In fact, we are seeing that information security is increasingly becoming a board-level discussion – a foundational component of the business strategy that's championed by the CEO and board. Cablevision exemplifies this.

"Our executives and board understand the importance of information security and express a keen interest in understanding what threats we face and what we are doing to mitigate our vulnerabilities," says Cablevision CSO Love. "Information security initiatives are readily embraced by both groups."

Executive support of security will only be wholly effective if it's communicated to the organisation, an approach that many telecoms have adopted. Consider this: 59% of telecommunications respondents said their organisation has a senior executive – a CEO, CFO, COO – who communicates the importance of security across the enterprise. And a similar number of respondents, 58%, said their organisation has a cross-functional team that coordinates and communicates security issues across the enterprise.

Combined, these actions demonstrate a new commitment to security, one that focuses on the involvement of top executives and the board to ensure that the company designs and implements an effective security program.

Another new approach is sharing information with others to improve security and gain intelligence on current threats. Among telecom respondents, 54% said they collaborate with others – including competitors – to improve security and reduce the potential for risks. Among them is Verizon Communications.

"I belong to the Telecommunications Security Association, an organisation that exists to share information and

includes members of the major carriers in the US, Canada, and the UK," says Mason of Verizon. "Adversaries, for instance, will try a scheme to infiltrate one operator until it works, and then use that same scheme to hit other telecoms. In this space, we are not competitive."

Technology safeguards, of course, are another foundational element to secure telecoms ecosystems against today's evolving threats. Operators are deploying solutions that augment threat detection and intelligence capabilities. Specifically, we've seen operators increase use of technology safeguards like intrusion-detection tools, asset-management tools, protection and detection solutions, patch-management tools, centralised user data storage, and more.

Effective security, from awareness to action

Today, information security is a discipline that demands advanced technologies and processes, a skill set based on counterintelligence techniques, and the unwavering support of top executives. As telecom operators become more similar to technology companies, they will face a raft of new challenges.

Core practices like employee awareness and training, policies and tools to reduce insider risks, and protection of data – including intellectual property – will need to be updated. The confluence of mobility, cloud, and social networking have multiplied risks, yet few operators have addressed these threats or deployed technologies that monitor user and network activity to provide insight into ecosystem vulnerabilities and threats.

These factors call for a new approach to security, one that's driven by knowledge of threats, assets, and adversaries. One in which security incidents are seen as a critical business risk that may not always be preventable, but can be managed to acceptable levels.

We call this model Awareness to Action. At its most basic, this approach comprises four key precepts: Security is now a business imperative, security threats are business risks, the most valuable information must be protected, and all activities and investments should be driven by comprehensive, current information about assets, ecosystem threats, and vulnerabilities.

This model will enable telecoms companies to effectively manage today's evolving threats, understand new threats that accompany a shifting business model, and prepare for the unknowable threats of tomorrow.

Footnotes

1 http://www.dhs.gov/news/2013/05/16/written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity-hearing.

2 *2013 US State of Cybercrime Survey*, co-sponsored by *CSO* magazine, CERT Coordination Center at Carnegie Mellon University, Federal Bureau of Investigation, PwC, and the US Secret Service, March-April 2013.

3 http://intelligize.com/wp-content/uploads/Managing-Risk-Better-2013.pdf.

Have an iPad?

If so, did you know that you can get this issue of Communications Review as an iBook? It's easy to do and it's FREE.

Visit the iTunes store and search for 'Communications Review' or visit www.pwc.com/communicationsreview and download it from our website. Now you can take Communications Review with you on your iPad and have access to additional audio and video on the topics in each issue.

Published in the USA for member firms of PricewaterhouseCoopers.

Code: CRV18N2