Communications Review / July 2015
Insights for telecom, cable, satellite, and Internet executives

As telcos go digital, cybersecurity risks intensify

pwc

As telecoms pivot toward a more digital future, they will very likely encounter entirely new types of cybersecurity risks to data, applications, and networks. Yet according to findings from The Global State of Information Security® Survey 2015, many telecommunications companies are not doing enough to address cyberthreats for today—or the future.

As the telecommunications industry continues its shift to a digital business model, organisations are recasting themselves as technology companies that offer a broad array of digital communications, connectivity, and content services.

They are racing to deliver not only high-quality and reliable communications services, but also to provide fresh content across a range of computing platforms to an expanding range of customers. Digitisation also has led to new products and services that are created and delivered in innovative ways, resulting in a raft of new collaborations, joint ventures, and strategic alliances across industries. At the same time, a slew of big deals are in the works, including mergers of telecommunications companies, multi-system operators, satellite television providers, and mobile communications networks. Some telecoms are acquiring businesses outside of their traditional scope to gain intellectual property and broaden their services.

Many of these changes are compounding network traffic and demanding that telecoms deliver enhanced capacity and quality of services—without raising fees to customers. That represents a formidable challenge as new entrants to the telecom market and lower pricing structures intensify competition and, in some cases, erode revenues.

Making matters more difficult: The frequency and scope of cybersecurity and privacy risks continue to mount. While breaches have typically targeted customer data, there is growing concern that ultra-sophisticated adversaries like nation-states, organised crime, and hacktivists will initiate attacks that disrupt services and even cause physical damage. A recent attack on a French television network provides an example that is uncomfortably close to home: In April, politically motivated hackers infiltrated a major television broadcaster, knocking 11 channels off the air and compromising websites and social media accounts.[1]

As telecoms pivot toward a more digital future, they will very likely encounter entirely new types of cybersecurity risks to data, applications, and networks. Yet according to findings from The Global State of Information Security® Survey[2] 2015 (GSISS),many telecommunications companies are not doing enough to address cyberthreats for today—or the future.

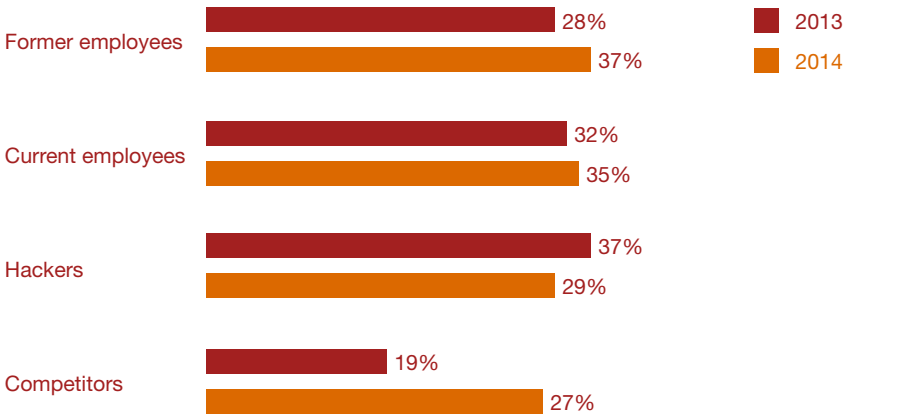
A decline in detected security incidents

Despite overwhelming evidence that cyber-risks continue to multiply across industries, the number of security incidents detected by telecommunications companies dropped almost 20% in 2014, according to the GSISS. (We define a security incident very broadly as any adverse incident that threatens some aspect of computer security.)

But a drop in incidents is not necessarily a good thing, especially when we peel back the data one layer. Security compromises are escalating globally, so a decline in detected incidents suggests that telecoms may be unable to identify intrusions. This seems increasingly likely as tech-savvy adversaries, particularly foreign nation-states and hacktivists, make it their business to carry out complex, sustained attacks without detection. When we look deeper at the GSISS results, we note in the broader survey that large organisations saw incidents increase 4% while incidents detected by smaller organisations decreased by over 20%. It may be the case that these smaller companies become the starting point for large complex attacks against larger companies.

And nothing keeps executives awake at night like the possibility of this type of multifaceted assault. Nation-states, in particular, often target critical infrastructure providers to steal intellectual property and trade secrets as a means to advance their own political and economic advantages or to possibly better position themselves to support Cyberwar activities. Among telecoms, incidents attributed to foreign nation-states skyrocketed 139%, while those ascribed to other foreign entities and organisations soared 66%. We also saw a 54% spike in compromises by hacktivists and activists, which often have ties to governments or ideologically motivated groups.

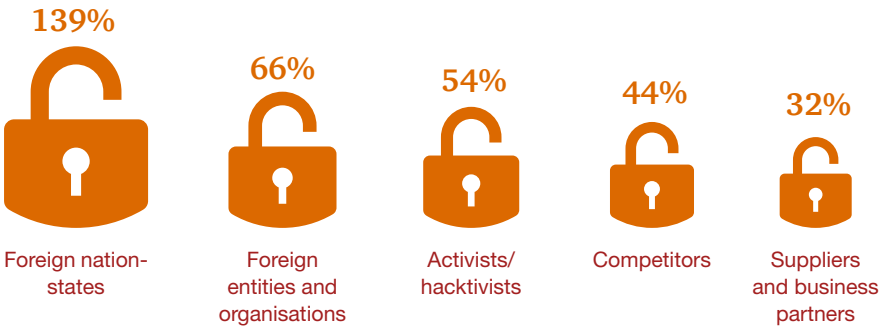
The most-cited sources of incidents



Source: PwC, *CSO* magazine, and *CIO* magazine, *The Global State of Information Security® Survey 2015*, September 2014.

Theft of information is not only costly, but can also jeopardise valuable customer relationships and brand reputation.

The fastest-growing sources of security incidents, increase over 2013



Source: PwC, *CSO* magazine, and *CIO* magazine, *The Global State of Information Security® Survey 2015*, September 2014.

Given the boom in activity by nation-states, it was not surprising to find a sizable increase in the loss of intellectual property and trade secrets. More specifically, we saw a substantial leap in theft of "hard" intellectual property such as strategic business plans, deal documents, and sensitive financial information.

Loss of employee and customer records, however, is still the most-cited consequence of security incidents. Telecoms, after all, often store a trove of detailed and valuable customer information, including call histories, website click streams, social media interactions, geolocation, and Internet Protocol addresses. Theft of this information is not only costly, but can also jeopardise valuable customer relationships and brand reputation.

While the overall number of detected security incidents declined in 2014, their financial impact took off in the other direction. Monetary losses attributed to security incidents soared 61% over 2013, and the number of respondents who reported losses of $1 million or more doubled. These findings suggest that sophisticated threat actors are refining their attack techniques to target more data. As a result, the clean-up is more costly.

Despite the spiralling costs of cybersecurity incidents, investment in information security slipped 6% in 2014, again led by smaller organisations. One explanation may be that telecoms boosted information security spending in 2013, and many businesses may have been hard-pressed to continue this level of investment. The spending slump also suggests that security executives are finding it difficult to prove the return on investment of information security outlays, particularly as global operators' revenues are beginning to stall. It seems likely, however, that recent high-profile attacks will impact budgets in the future. That's something we plan to keep an eye on.

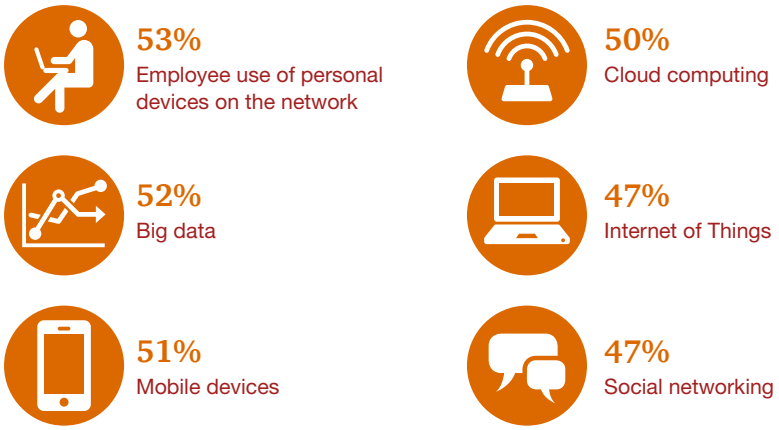
The rewards and risks of the cloud, devices, and data

Digitalisation is generating seismic changes in how telecommunications companies deliver products and services, manage their operations, and interact with customers. In particular, the nexus of cloud computing, the Internet of Things, and Big Data analytics is creating a panoply of new services, customers, and partnerships. In many cases, however, telecommunications businesses are not addressing the risks that inevitably accompany this degree of transformation.

Cloud computing: Over the past decade, consumer and business adoption of cloud computing has been perhaps the greatest catalyst for change and digitisation. As it has become mainstream, the cloud has rewritten the rules of how businesses and consumers manage, use, and think about technology.

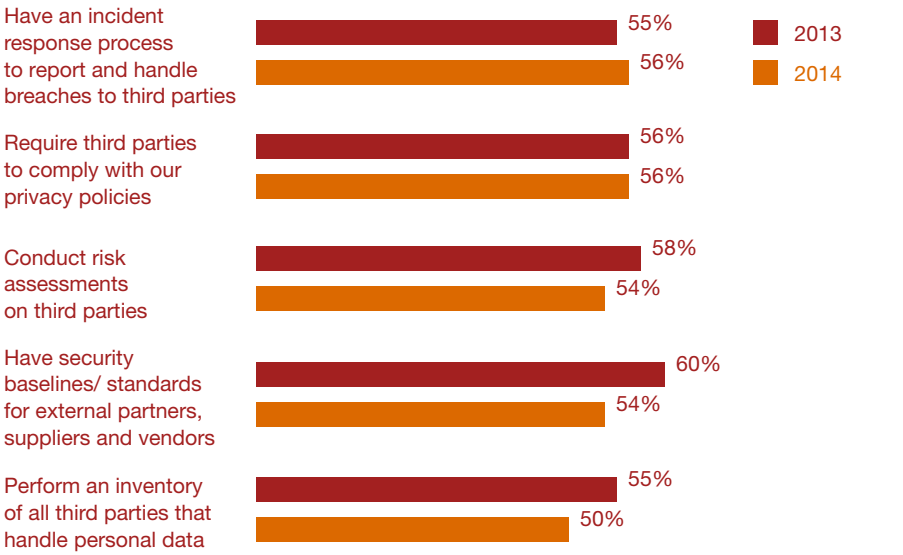
In 2014, 60% of telecommunications respondents said they employ some form of cloud computing, up from 50% in 2013. Increasingly, telecom operators are leveraging cloud services to improve efficiencies in business operations, roll out new applications and services, and store and distribute content. Many see the cloud as a solution to deliver expanded network capacity and secure, reliable, and inexpensive communications and content.

Security strategies for evolving technologies, 2014



Source: PwC, *CSO* magazine, and *CIO* magazine, *The Global State of Information Security® Survey 2015*, September 2014.

Key safeguards for third-party security and privacy



Source: PwC, *CSO* magazine, and *CIO* magazine, *The Global State of Information Security® Survey 2015*, September 2014.

The benefits of cloud services continue to grow as the technology matures, but so do risks. We found several scenarios that may raise concern. Consider, for instance, that only 50% of telecom respondents have a security strategy for cloud computing. And "shadow IT"—the purchase of cloud services by business leaders without involvement of IT—can increase risks because the cybersecurity practices of cloud providers may not be adequately vetted. And even when IT is involved, a lack of due diligence is common: According to the GSISS, only 54% of telecoms said they perform risk assessments on third-party vendors like cloud providers.

Certain technologies that are key to cloud-based security are also lacking. Consider that only 53% of respondents said they have processes for risk-based authorisation and authentication, and fewer (49%) have implemented identity and access management tools. We also found that people skills are often not prioritised. Staff education should form the backbone of every information security program, so it was worrisome to learn that only 54% of telecom respondents have a security awareness and training program, a decline over the year before. Slightly more (56%) said they require employees to complete training on privacy policies and practices.

The Internet of Things: Imagine a world in which everyone and everything are connected. Then consider the potential for growth—and disruption—for telecommunications organisations.

As more devices are interconnected and share data, the Internet of Things will open a fire hose of network traffic and data volume. By the year 2020, Gartner estimates that 25 billion devices will be interconnected via the Internet.[3] Telecoms stand to gain unique business opportunities because these billions of devices will be largely connected via the Internet, cellular, and Wi-Fi networks.

What's more, the digitally connected home provides a natural entry point for telecoms to develop and deliver new services and products. Already, some telecommunications companies offer home automation, physical security, and remote control of lighting and thermostats as add-ons to basic services. Wireless carriers, in particular, can play an important role because the smartphone will likely serve as the remote control of the digital home.

Business-to-business opportunities are also thriving on the Internet of Things, creating a constellation of new partnerships and relationships. In the US, AT&T and IBM are developing a program for city governments and midsize utilities that will integrate and analyse data from connected devices to help improve urban planning and better manage utilities equipment.[4] In Germany, Deutsche Telekom has launched an initiative called Industry 4.0 that supports the digitisation and automation of

industrial manufacturing, as well as logistics, customer service, and after-sales support.[5]

The business opportunities are practically boundless, but so too are potential cybersecurity risks. The reason? As more devices are connected, exponentially more data will traverse interconnected business ecosystems and will be in jeopardy of compromise. It's a threat that many telecom companies seem to recognise: 47% of respondents said they have implemented a security strategy for the Internet of Things, and an additional 26% said they are implementing one.

More specifically, securing the Internet of Things will demand that businesses deploy robust authentication to maintain the integrity of networks, applications, and data. It did not inspire confidence, therefore, to learn that just 56% of respondents employ multi-factor authentication.

Big Data: Like the Internet of Things, Big Data is compounding the volume of information that is shared and potentially at risk. It also introduces new imperatives for data privacy—an issue that many telecoms do not rigourously address.

As noted above, telecommunications companies—wireless carriers, in particular—store tremendous amounts of very detailed information about customers. If not properly managed, the risks of compromise and costs of maintaining data can be prohibitive.

Consider, for instance, that only 53% of telecom respondents said they limit collection, retention, and access of personal information, down from 57% last year. Only half (50%) said they have conducted an inventory of all third parties that handle personal data of customers and employees, a number that also declined over the year before.

Telecoms that use Big Data analytics, whether internally or as a service offering to other businesses, should frequently assess and update their privacy programs to keep pace with evolving customer demands and ensure compliance with disparate privacy regulations. Yet we found that approximately 40% of survey respondents do not review their privacy policies on an annual basis. What's more, just 56% said they require third-party vendors to comply with their privacy policies.

Cashing in on mobile payments

Some telecommunications companies are preparing to move into the Wild West of digital opportunity: mobile payment systems.

Mobile payments aren't exactly new, but the ecosystem is quickly evolving as new partnerships are formed among a range of telecoms, technology companies, banks, and retailers. It's also a booming market: Mobile payment transactions in the US are forecast to climb to $8.95 billion this year and reach $118.01 billion in 2018, according to research company eMarketer.[6]

Long before Apple Pay was announced in 2014, telecoms in emerging markets took the lead in implementing mobile payments. The M-Pesa system was launched in Kenya in 2007 by Vodafone; it now has 17 million active users in Africa, India, and Europe.[7] Other telecoms that operate their own mobile payment systems include Deutsche Telekom and Orange.

While mobile payment systems typically comprise multiple partnerships, telecoms hold a distinct advantage in that they operate the network on which the financial transactions are transmitted and have an established, trusted brand with a reputation for effective cybersecurity. Some also sell the devices on which transactions are made.

As more digital payment systems are introduced, they may bring unanticipated security risks and broaden the cyberattack vector. For example, MCX said that email addresses of participants in a pilot for its CurrentC payment system were breached last year.[8] Apple Pay also fell victim to fraudsters when criminals entered stolen payment card information into iPhones and made fraudulent purchases.

More than half (54%) of telecom respondents said they have purchased cybersecurity coverage.

Strategic initiatives to improve cybersecurity

While implementation of some core security safeguards slipped in 2014, the news is not all bad. We saw a noticeable uptick in adoption of new strategic initiatives like risk-based information security frameworks, external collaboration to improve security, and purchase of cybersecurity insurance.

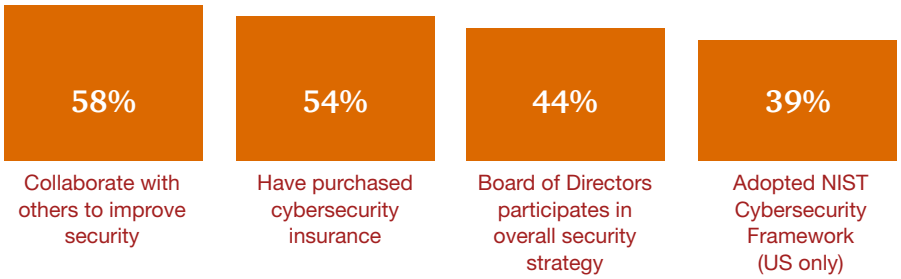
In the US, many telecoms are embracing the National Institute of Standards and Technology (NIST) Cybersecurity Framework to more closely link technologies, processes, and personnel skills with their risk-management activities. The NIST Framework, which targets critical infrastructure providers and suppliers, has been adopted by 39% of US telecom respondents, a rate that is higher than most other industries. An additional 17% said adoption of the Framework is a future priority.

In addition to improving risk-based cybersecurity, the Framework also aims to create a common language to facilitate collaboration and communication among internal executives and external industry and government organisations. In the past several years, sharing of threat intelligence and response tactics has become an indispensable tool to advance cybersecurity, one that the telecom sector has readily adopted. This year GSISS results show that 58% of telecom respondents said they work with others to improve security, slightly higher than the overall survey sample.

Internally, it has become increasingly critical that businesses communicate with their Board of Directors on cybersecurity oversight. A comparatively high number of telecom respondents (44%) said their Board participates in the overall information security strategy, and 30% said directors are involved in reviews of security and privacy risks. While telecoms engage their Boards to a greater degree than many other industries, we believe that all Boards should be involved in cybersecurity oversight.

Risks will never be completely eliminated, however, and many organisations are finding that cybersecurity insurance can help mitigate financial losses of cyberattacks. In fact, recent victims of high-profile breaches reported they have recovered tens of millions of dollars in mitigation costs through insurance coverage. It's no wonder, then that more than half (54%) of telecom respondents said they have purchased cybersecurity coverage. We expect the numbers of companies that take out policies will continue to climb in the years ahead.

Adoption of strategic initiatives, 2014



Source: PwC, *CSO* magazine, and *CIO* magazine, *The Global State of Information Security® Survey 2015*, September 2014.

Building a future with cybersecurity

Digitisation has transformed how telecoms operate, provide services, and communicate with customers. This disruptive business ecosystem, combined with increasingly frequent and sophisticated cyber-risks, demands a commitment to cybersecurity that focuses on highly trained personnel, up-to-date processes, and the right tools to detect, analyse, and respond to threats.

A robust cybersecurity practice also can create competitive advantages by boosting customer trust in the organisation's brand and reputation, giving the company a leg up in launching new services like mobile payments. Forward-thinking telecommunications organisations are also starting to market cybersecurity services to other businesses. Singapore Telecom, for example, recently announced plans to build out its cybersecurity capabilities by purchasing the assets of Trustwave, a US company that provides managed security services.[9]

As the telecommunications industry reinvents itself and cyber-risks evolve, cybersecurity will continue to be top of mind for telecom executives, Boards of Directors, and consumers alike. It is an all-encompassing, persistent risk issue that is critical to the resilience and revenues of today's increasingly digital telecoms and retaining connected customers.

Endnotes

1 CSO, *Islamist hackers take French broadcaster TV5Monde off air*, April 9, 2015

2 PwC, *CSO* magazine, and *CIO* magazine, *The Global State of Information Security® Survey 2015*, September 2014

3 Gartner, *Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015*, November 11, 2014

4 IBM, *AT&T And IBM Join Forces To Deliver New Innovations For The Internet of Things*, February 18, 2014

5 Deutsche Telekom, *Everything is getting smarter*, accessed May 29, 2015

6 eMarketer, *How Popular Are Mobile In-Store Payments?* April 30, 2015

7 CNN.com, *Africa's mobile money makes its way to Europe with M-Pesa*, January 5, 2015

8 MCX, *10/28 email incident report*, accessed May 29, 2015

9 PC World, *SingTel acquires Trustwave for managed security services*, April 7, 2015

About the authors

Thomas Tandetzki

Thomas is a Partner with PwC Germany and also serves as PwC's Global Communications Industry Leader.

For more information, contact Thomas
by phone at +49 211 981 1105 or
by email at thomas.tandetzki@de.pwc.com

Mark Lobel

Mark is a Partner in PwC US's Security and Entertainment & Media and Communications practice.

For more information, contact Mark
by phone at +1 646 471 5731 or
by email at mark.a.lobel@us.pwc.com.