Assessing the strength of your security operating model
Assessing the strength of your security operating model

Retail stores, software companies, the U.S. Federal Reserve — it seems like every day we hear about a new IT security breach threatening to destroy a company or agency’s reputation. Everyone is vulnerable. At the same time, ubiquitous vulnerability means that opportunities are everywhere to inspire confidence through security.

Evolving technologies have brought with them evolving threats and too many companies are running to stand still, let alone catch up. While the telecom industry has responded to threats with increased investments in security, attackers have done better.

The competitive landscape for telecom operators is changing, driven by consolidation in the market, a need to identify new revenue streams to maintain average revenue per user (ARPU) and pressure to improve net promoter scores (NPS). This has driven the adoption of new business models with complex eco-systems based on partnerships and joint ventures. And with so much data flowing between partners, the places ripe for attack have increased exponentially. Security can no longer remain the domain of IT functions; it must be a concern for everyone, from CEOs down to rank-and-file employees. It is no longer about protecting just the perimeter. Effective security must be woven into all levels of business.

Data cannot all be protected equally; companies must constantly prioritize and assess risks. And while that means new responsibility, it also brings with it new opportunity. If losing trust is the risk in the new security landscape, providing it is the opportunity. As potential clients feel more and more threatened by the possibility of a security breach, they are increasingly looking for providers who can offer increased assurance that their data and systems are safe. Companies that appropriately invest and incorporate security into their entire culture can stand above the rest by inspiring confidence.
**Everyone at Risk**

The threat is real — 93% of large organizations and 87% of small businesses had a security breach in the last year. Further, in PwC’s 17th annual CEO Survey, *Fit for the future*, 54% of telecoms respondents said they are either ‘somewhat concerned’ or ‘extremely concerned’ about cyber threats including lack of data security.

For telecoms operators, the biggest single threat is from the inside. Current employees were suspected in 32% of cases, while former employees were suspected 28% of the time. And these breaches are no longer just hackers having fun and seeking a challenge. Instead, the attackers are organized, funded and seeking monetary gain. For telecoms operators, the biggest impact of security breaches last year was the compromise of customer or employee information.

As telecoms operators increasingly diversify into cloud services, acquire or merge with other companies, and collaborate and compete with app-based technology, the risk landscape grows. Every time they work with another company — as a partner, as a supplier, as a service provider — they acquire that company’s security risks. Every piece of data and every service managed through the cloud opens new doors to threats. And while half of telecoms operators use cloud services, only one-fifth include the cloud in their security policy.

Telecommunications is a particularly risky sector. While cyber security risks occur in a lot of ways, data breaches often capture much public attention and publicity. Telecoms have access to an enormous amount of data, so if that data is compromised, the public blame could fall on them, whether they are responsible or not. Telecoms operators are still critical infrastructure — they provide the pipes through which data travels, from a credit card company to its clients, from a mobile payment app to a retailer. If something happens to that data along the way, people may blame the pipes.

And as telecoms operators diversify into new technology offerings — over the top (OTT), machine-to-machine (M2M), near field communications (NFC), mobile payments — each presents different and ever-changing security challenges. Such offerings must be secured for today’s risks, but also those that come tomorrow and next year. Those technologies are also elevating what’s at stake in a security breach. Instead of identity theft or monetary losses, if an M2M communication is hacked, a car’s safety system could be compromised or a medical device could stop working.

All of these elevated risks come as companies are increasingly allowing bring your own device (BYOD) policies and as people are turning more and more to their mobile devices for a variety of services. But these individuals aren’t taking security into their own hands. Individual users rarely take the necessary precautions to secure their handsets. They expect the security to come from their companies and their telecoms providers.

---

1 PwC 2013 Information Security Breaches Survey
3 PwC’s 2014 Global State of Information Security Survey
4 Global State of Information Security Survey, PwC, September 2013
High stakes and ample opportunities

Security breaches damage reputations and destroy trust—both are vital ingredients for success in the digital age. Lost trust translates to lost business: 61% of consumers would stop using a company’s product or services if an attack resulted in a known breach.6

But trust also provides an incredible opportunity for telecoms operators. The value of security has changed, for both individuals and companies. For example, security threats have made some companies start to question the use of cloud-based services. A telecom operator that can provide such services securely and inspire confidence among its consumers holds a competitive advantage.

The field is wide-open for leaders—while 53% of telecom respondents in PwC’s 2014 Global State of Information Security Survey said they are “frontrunners” in their security practices, only 18% actually are.7

Both individual consumers and large companies have begun to view information security differently. Telecoms operators need to respond by implementing a holistic security strategy across their business and embedding security into the fabric of their systems, networks, and applications. They also need to start articulating their ability to manage security risk to customers and potential customers, and clearly define what they can realistically deliver and what customers have to take responsibility for. That is where trust begins.

Trust grows as customers and clients believe their data and transactions are safe, that systems and processes will be available when needed, and that identity and privacy are protected (see chart below).

Trust takes a long time to build but can be lost in an instant.

The new trust dynamic: Opportunity + Trust = Growth

By building trust you will be able to maximise your growth potential and manage the risks in the opportunities available in the digital age.

---


7 PwC, The global state of information security survey 2014, Telecommunications industry summary, page 12
http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml

Source: Building Digital Trust — The confidence to take risks, PwC, 2014
New strategies for sound security

Many telecoms operators can find they are over reliant on technology, such as application firewalls and encryption, which no longer protect against many threats. And many lack security safeguards that monitor data and assets, such as behavioural profiling and monitoring and asset management tools, which can provide ongoing intelligence into security threats. Leaders in the telecom industry have implemented these more valuable safeguards; all telecoms operators should do so.

But that is just the beginning. Cyber security isn’t just about technology. It is also about people, systems, processes and a business culture aimed at creating a secure environment. Companies need to make sure their employees understand their responsibility in building security. It starts at the top with CEOs and boards. Those top officials need to establish a clear risk appetite based on their situation and must regularly assess and monitor their risks.

Not all assets are equal, so security investments to protect those assets have to be targeted to bring the maximum ROI. Safeguarding everything at the highest level is not realistic, possible or worth the cost. Breaches in some areas may be troubling, while in others they can destroy a business. Asset protection can no longer be a one-size fits all approach. Instead, data, transactions and operations must be prioritized and protected accordingly. Some security incidents have to be seen as a business risk and managed.

When IT incidents or disasters do occur, companies should be fully prepared and able to respond quickly.

Trust takes a long time to build but can be lost in an instant.
This risk management isn’t static—threats come and go, increase and decrease, as does a board’s risk appetite, so managing risk has to be an on-going process. Having adequate, on-going threat intelligence is key to this management. Today’s security is not just a capital investment—it is an investment that must be made every year to reap the benefits.

The ever-changing security landscape has also brought with it new and evolving regulations that vary across the globe. Companies that comply with individual regulations as they come into effect for each system or product as it comes online can find themselves with inefficiencies, overlapping controls or even contradicting practices. Regulation compliance must be implemented comprehensively and on a company-wide basis.

Companies must also assess and manage the security risks of their partners and suppliers, and require those partners and suppliers to adhere to their security practices.

We believe that there is a need to view security through a series of interconnected lenses. Our rounded approach (see chart below) is designed to provide confidence, in people, technology and connections, how risk is managed, priorities set and how you respond to an incident or during a crises. This will enable you to develop a cyber security strategy to build confidence in your digital future.

You can’t secure everything
We help you set the right priorities.
• Enterprise security architecture
• Protect what matters
• Strategy, organisation and governance
• Threat intelligence

It’s not if but when
We help you build an intelligence-led defence, enabling rapid detection and containment.
• Continuity and resilience
• Crisis management
• Incident response and forensics
• Monitoring and detection

Fix the basics
We help you use technology to your advantage, deriving maximum return from your technology investments.
• Identity and access management
• Information technology, operations technology and consumer technology
• IT security hygiene
• Security intelligence and analytics

Seize the advantage
We help you exploit digital opportunity with
• Digital trust is embedded in the strategy
• Privacy and cyber security legal compliance
• Risk management and risk appetite

Their risk is your risk
We help you understand and manage risk in your interconnected business ecosystem.
• Digital channels
• Partner and supplier management
• Robust contracts

People matter
We help you build and maintain a secure culture, where people are aware of their critical security decisions.
• Insider threat management
• People and ‘moments that matter’
• Security culture and awareness

Source: Cyber security: building confidence in your digital future, PwC, November 2013
On a broader scale, telecoms operators should work with not only their partners, but also their competitors to improve security. Many telecoms operators are not doing so, fearing their competitors will use it against them. But collaboration allows for faster adaption to manage evolving risks (see chart below). Companies can’t keep security breaches to themselves anymore. They should collaborate with industry working groups and public/private partnerships.

<table>
<thead>
<tr>
<th>Adversary</th>
<th>Motives</th>
<th>Targets</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nation state</td>
<td>• Economic, political, and/or military advantage</td>
<td>• Trade secrets</td>
<td>• Loss of competitive advantage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sensitive business information</td>
<td>• Disruption to critical infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Emerging technologies</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Critical infrastructure</td>
<td></td>
</tr>
<tr>
<td>Organised crime</td>
<td>• Immediate financial gain</td>
<td>• Financial/payment systems</td>
<td>• Costly regulatory inquiries and penalties</td>
</tr>
<tr>
<td></td>
<td>• Collect information for future financial gains</td>
<td>• Personally identifiable information</td>
<td>• Consumer and shareholder lawsuits</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Payment card information</td>
<td>• Loss of consumer confidence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Protected health information</td>
<td>• Financial loss</td>
</tr>
<tr>
<td>Hacktivists</td>
<td>• Influence political and/or social change</td>
<td>• Corporate secrets</td>
<td>• Disruption of business activities</td>
</tr>
<tr>
<td></td>
<td>• Pressure business to change their practices</td>
<td>• Sensitive business information</td>
<td>• Brand and reputation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Information related to key executives, employees, customers and business partners</td>
<td>• Loss of consumer confidence</td>
</tr>
<tr>
<td>Insiders</td>
<td>• Personal advantage, monetary gain</td>
<td>• Sales, deals, market strategies</td>
<td>• Trade secret disclosure</td>
</tr>
<tr>
<td></td>
<td>• Professional revenge</td>
<td>• Corporate secrets, IP, R&amp;D</td>
<td>• Operational disruption</td>
</tr>
<tr>
<td></td>
<td>• Patriotism</td>
<td>• Business operations</td>
<td>• Brand and reputation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Personnel information</td>
<td>• National security impact</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Cyber security: building confidence in your digital future, PwC, November 2013

**Conclusion**

Cyber security is no longer just an IT challenge. It is a complex and constantly evolving strategy that should be part of a company’s entire business ecosystem.

Telecoms operators and the companies they serve are increasingly moving internal services to the cloud, using external providers for a variety of other services, and adopting new technologies. Connectivity and collaboration is now how business is done, opening up an entirely new world of cyber security threats.

Those new risks offer a new set of rewards. Telecom operators that respond to this new business reality with strong security strategies, offering trust and safety in an uncertain world, will thrive. Our security experts can help companies develop and implement those strategies, allowing confidence to grow.
To have a deeper conversation about how this subject may affect your business, please contact:

**Pierre-Alain Sur**  
Global Communications Leader  
New York  
+1 646 471 6973

**Chris Oxborough**  
Partner, PwC UK  
London  
+44 2072 124195

**John Ridley**  
Director, PwC UK  
London  
+44 2078 041552