Cyber risk: Why cyber security is important

Cyber risk is now firmly at the top of the international agenda as high-profile breaches raise fears that hack attacks and other security failures could endanger the global economy.

The *Global Risks 2015* report, published in January by the World Economic Forum (WEF), included this rather stark warning: "90 percent of companies worldwide recognize they are insufficiently prepared to protect themselves against [cyber attacks]."

Cyber crime costs the global economy over US$400 billion per year, according to estimates by the Center for Strategic and International Studies. In 2013, some 3,000 companies in the United States had their systems compromised by criminals, the Center reports.

High-profile US retailers Target and Home Depot were among many organizations that lost customer data and credit card information. In other companies, cyber criminals stole money from accounts, carried out industrial espionage and in some cases even took over company systems and demanded ransom money to unlock them.

It's not surprising that governments and businesses around the world are searching for better cyber defense strategies. The European Network and Information Security Agency held a cyber security exercise in October 2014, involving 29 countries and more than 200 organizations, including government bodies, telecoms companies, energy suppliers, financial institutions and Internet service providers.

The tests included simulating more than 2,000 separate incidents: denial of service attacks, website defacements, access to sensitive information and attacks on critical infrastructure. Software and hardware failures were judged the biggest security threats.

In February, President Barack Obama addressed the Summit on Cybersecurity and Consumer Protection at Stanford University. It was attended by senior US political leaders, CEOs and representatives from computer security companies, major retailers, law enforcement and technical experts, to "collaborate and explore partnerships that will help develop the best ways to bolster our cyber security."

There is clearly still much work to be done, and the people behind the attacks have a significant head start. For those playing catch-up, cyber security has become a matter of urgency.

The consequences of cyber crime

Cyber attacks fall into two broad categories: breaches in data security and sabotage. Personal data, intellectual property, trade secrets and information relating to bids, mergers and prices are tempting targets for a data security breach. Sabotage can take the form of denial of service attacks, which flood web services with bogus messages, as well as more conventional efforts to disable systems and infrastructure.

In addition to commercial losses and public relations problems, disruption of operations and the possibility of extortion, cyber attacks may also expose an organization to regulatory action, negligence claims, the inability to meet contractual obligations and a damaging loss of trust among customers and suppliers.

Most cyber crime incidents go unreported, and few companies come forward with information on their losses. That is not surprising given the risk to an organization's reputation and the prospect of legal action against those that own up to cyber crime. Few of the biggest cyber criminals have been caught—many have yet to be identified.

A significant proportion of cyber crime also goes undetected, particularly industrial espionage where access to confidential documents and data is difficult to spot. There is a danger that a business might trade at a disadvantage for months or even years as a result of a continuing, but undetected, security breach.

"Criminals operate across borders, so must companies and the experts that assist them, including their lawyers," says Bertrand Liard, a Paris-based partner at White & Case. "Responding to cyber attacks requires both a global vision and

a fine knowledge of local regulations and law enforcement agencies."

Vulnerability is on the rise

Cyber crime is only likely to increase, despite the best efforts of government agencies and cyber security experts. Its growth is being driven by the expanding number of services available online and the increasing sophistication of cyber criminals who are engaged in a cat-and-mouse game with security experts.

Technical innovation throws up new online dangers. For example, the migration of data to third-party cloud providers has created a centralization of data and therefore more opportunities for criminals to misappropriate critical information from a single target attack. Similarly, the emphasis on mobile services has opened up corporate systems to more users—multiplying the opportunities to penetrate security measures.

Applications that involve the collection and analysis of data in large quantities—so-called Big Data—put additional pressure on security managers. Mountains of sensitive data about buyer decisions, their habits and other personal information must be kept safe, but until recently security was not a top priority in systems handling Big Data.

The development of an Internet of Things, which enables communication between machines, raises the possibility of appliances being manipulated by hackers. The widespread use of machine-to-machine (M2M) communication is only likely to boost the possibility of information misuse.

Much of the world's critical infrastructure, controlling services such as power generation, transport and utilities, already depends on M2M. Protecting the networks that carry the communications that control these services is vital, especially since decision making is often done without human involvement.

Countering cyber risk

"Cyber security is regarded as a board-level responsibility," says Detlev Gabel, a partner at White & Case in Frankfurt and leader of the Firm's Data, Privacy and Cyber Security Group. "Similar to other compliance areas, board directors can be held liable for not discharging their duty to prevent harm to the corporation. In performing their oversight role, directors should stay informed about the corporation's cyber security defenses. They must ask what the risks are and

determine what needs to be done to mitigate them. In today's connected world, it is unfortunately becoming a question of 'when' rather than 'if' some sort of data breach will occur."

Furthermore, under guidance from the US Securities and Exchange Commission, public companies are required to disclose the material risks they face from cyber attacks and include specific detail to enable an investor to assess the magnitude of those risks.

US companies are also required to consider disclosure about the potential costs associated with preventing cyber attacks and any contingent liabilities or asserted claims related to prior breaches. In sum, a failure to make adequate disclosures can lead to additional liability in the event of a cyber attack.

There is no shortage of advice available to organizations to help them assess risks and develop suitable plans to counter them. Governments around the world are developing cyber security guidelines.

Last year, at the behest of President Obama, the National Institute of Standards and Technology (NIST) in the United States issued a Framework for Improving Critical Infrastructure Security. Critical infrastructure not only includes energy supply networks and telecommunications, but financial services and retail facilities as well.

The Framework is a set of standards and best practices drawn up with the input of thousands of security experts and designed to help organizations manage the risks of a cyber security breach. With the aid of the Framework, they chart their current security profile, work out what profile they should be aiming for and create a plan for reaching it.

"Similar to financial and reputational risk, cyber security risk affects a company's bottom line. It can drive up costs and impact revenue. It can harm an organization's ability to innovate and to gain and maintain customers," warns NIST.

The UK intelligence agency, Government Communications Headquarters (GCHQ), which provides advice and services to protect national voice and data networks, estimates 81 percent of UK businesses have experienced some kind of security breach. To help stem the tide, the organization has published detailed guidance for businesses, "10 Steps to Cyber Security."

The critical first step is to establish an information risk management regime that identifies the security risks it faces and the policy for dealing with them. Businesses should protect their information and communications technology by adopting standard security measures and managing how the systems are configured and used. They should also disable unnecessary functions and keep security patches up to date.

Malware protection is an important security consideration. Businesses should not only have policies that cover email, web browsing and the use of personal devices, but also install antivirus software and regularly scan for malware.

Networks are often a weak point in cyber defenses, so it's crucial for businesses to follow recognized network design principles and ensure all devices are configured to the security standards they have adopted.

Removable media policies that control the use of media for the import and export of information are vital. Not only should removable media be scanned for malware, but the type of media and the sort of information that can be transferred should be limited.

47

American states have enacted laws that require security breaches involving personal data to be reported to the authorities. Many countries in the European Union have introduced similar regulations.

Users should only be given the privileges they need to do their job. Accounts used by system or database administrators should not be used for high-risk user activities. User activity should be monitored; particularly those involving access to sensitive information and account actions such as changing passwords and deleting accounts.

The same can be said for vendors, who are often not perceived as a threat or lacking in security measures of their own—many breaches in recent years were via vendors.

"The point is you can't just draft all these fantastic policies and apply them internally, but then not be strict with all vendors," says Daren Orzechowski, a partner at White & Case in New York. "You need to ensure that these cyber policies are also imposed on vendors by way of a contract."

Equally, security policies should be part of employment terms and conditions. All users should receive regular training on the cyber risks they face.

Businesses are also urged to scan inbound and outbound traffic continuously to detect suspicious activity. They should also monitor all ICT systems using specialized intrusion detection and prevention systems.

Legal aspects of cyber risk

Governments are tightening laws to ensure organizations take greater responsibility for cyber security and report cyber breaches. The reporting of breaches is important in that it enables government agencies to take action to strengthen security, allows individuals to mitigate harm and encourages organizations to adopt effective security measures.

In the United States, 47 states have enacted laws that require security breaches involving personal data to be reported. The US Congress is also considering various proposals, including one from the Obama Administration, concerning a national breach notification law. The Data Security and Breach Notification Act of 2015 is a companion to the Consumer Privacy Bill of Rights Act of 2015 unveiled by President Obama in February, governing the collection and dissemination of consumer data. According to a White House spokesperson, these will "provide customers with more control over their data, companies with clearer ways to signal their responsible stewardship over data, and everyone with the flexibility to continue innovating in the digital age."

While such legislative moves are welcome, they have their critics: fines are not particularly prohibitive and it's not clear how they would be enforced, and businesses would be allowed to draft their own codes of conduct, leaving room for loopholes.

The European Union and several of its member states have introduced similar regulations, some of which are specific to particular industries, with the result that organizations operating across different legal jurisdictions have the added burden of making sure they comply with the different laws.

> **"You can't just draft all these fantastic policies and apply them internally, but then not be strict with all vendors"**
>
> Daren Orzechowski, partner, White & Case, New York

Meanwhile, the EU is developing a proposal for a General Data Protection Regulation to replace and harmonize current data protection legislation. The new regime would require organizations to report data breaches promptly to both the competent authorities and the affected individuals. If it were up to the European Parliament, as one of the legislative bodies deciding on the proposal, failure to comply with this requirement could lead to penalties equivalent to 5 percent of an offender's global turnover.

Preparing for a breach in security, therefore, is particularly important when incidents can result in fines, legal action or measures by government agencies. An effective plan reduces the risks of financial losses and damage to an organization's reputation while ensuring compliance with the relevant legal requirements.

"Looking proactively, you should get input from IT professionals, lawyers, technologists and privacy experts. And it only makes sense that the same team that builds the plan should help prepare for a problem," says Orzechowski.

In the event of an incident, Orzechowski recommends that a lawyer be included on the team in charge of any fact-finding mission so that the company can claim attorney-client privilege and work-product protection. These protections, at least under US law, might prevent the disclosure of information that could be detrimental to their client if future litigation arises following an incident.

Conclusion

Cyber security is one of the most urgent issues of the day. Computer networks have always been the target of criminals, and it is likely that the danger of cyber security breaches will only increase in the future as these networks expand, but there are sensible precautions that organizations can take to minimize losses from those who seek to do harm.

With the right level of preparation and specialist external assistance, it is possible to control damages, and recover from a cyber breach and its consequences.