BY PAOLO BORGHESI,
JON RIGBY, DAVID WHITE
AND JIM HART

GUARDING against cyber threats

In a world awash in cyber threats, partners and suppliers can be the vulnerable points that cyber criminals exploit to gain access to systems. Those challenges will get worse before they get better as supply networks become ever more complex. As a matter of urgency, business leaders must proactively balance cyber risks against opportunity, growth and profitability, starting with a clear-eyed view of the size and scale of the risks. Then it's time to set concrete expectations for suppliers. Here's a snapshot of the discussions you should be having right now.

Not too long ago, Goodwill Industries found that its customers' payments data had been breached by cyber criminals. Data from 868,000 payment card accounts was stolen. The entry point for the attack? Hackers had used malware to penetrate a third-party vendor's systems.

A year earlier, Target made news when it suffered a huge and highly publicized breach in which data from 110 million customers and 40 million payment cards was stolen. The national retailer's systems were initially breached via a connection with one of its vendors, an HVAC provider.

Goodwill and Target are by no means alone. Cyber breaches are proliferating year over year, affecting the confidentiality, integrity and availability of data; recent research by IBM indicates that just between 2014 and 2015, the number of such security incidents increased by 64%. These statistics probably reveal just the tip of the iceberg; they refer only to the security incidents that are detected and declared.

Retail and telecommunications companies are some of the most common victims of such attacks, but now, the Internet of Things (IoT) is also making manufacturing and production just as vulnerable. More broadly, ancillary sub-systems have proved alarmingly open to attack; there are well-publicized

Paolo Borghesi is vice president, Cyber Security Strategy, at AlixPartners LLP. He can be reached at pborghesi@alixpartners.com. Jon Rigby is director of AlixPartners' Cyber practice. He can be reached at jrigby@alixpartners.com. David White is director of legal services at AlixPartners. He can be reached at dwhite@alixpartners.com. Jim Hart can be reached at jim_hart_99@hotmail.com.

stories of car engine-control computers being accessed by hackers via CD players and tire pressure monitors. Seemingly innocuous devices have been used in massive denial-of-service disruptions; these attacks recently wreaked havoc on Amazon, BBC, CNN, Netflix and other household-name organizations when Internet-connected devices, such as printers, cameras and baby monitors, were hacked.

More cyber attacks—whether inadvertent or malicious—are coming from insiders: employees, contractors, consultants, suppliers and partners.

At least as worrying: more of the attacks—whether inadvertent or malicious—are coming from insiders: employees, contractors, consultants, suppliers and partners. In nearly two-thirds of incident response investigations, a major component of IT support was outsourced to a third party, according to the 2013 Global Security Report from Trustwave, a security services provider. No business operates independently of partners or suppliers: A company's connections with those entities ranges from the exchange of purchase order details via e-mail or some other electronic exchange, to vendor-controlled facility management systems, to integrated design and production environments—all of which are potential security vulnerabilities. The push for greater efficiency and more innovation opportunities adds to the pressure to integrate with others in the supply chain, often without due consideration of the concomitant rise in business risk.

Of course, there is no shortage of techniques and technologies to minimize that risk. Even in the most complex businesses, it is possible to segregate information to allow for complete trust and openness with suppliers in one business process while blocking access to other information. The implementation of these safeguarding measures is not just an IT function; it requires business leaders to consider their information requirements as closely as they consider their physical pipeline, and it calls for commercial staff to write contracts that allow oversight of suppliers' information security.

It is not that business leaders aren't aware of the challenges—or aren't trying. More than two-thirds (69%) of public company board members report that their board is "more involved" with cyber security than it was 12 months earlier, according to a survey by BDO. That still isn't enough. Despite this increase in awareness, just one-third (34%) of corporate directors report that they have documented and developed solutions to protect their business's critical digital assets. Clearly, more must be done.

In practice, business executives should adopt a risk mindset. Few of the useful risk-mitigation techniques can be truly effective if business leaders fail to balance the trust they place in partners and suppliers against the risks to their bottom line and value. They must weigh opportunity, growth and profitability against risk and make conscious investment decisions based on their business judgment. It is incumbent on executives and directors to educate themselves about cyber security and empower themselves to make informed decisions.

The obvious part of that imperative is to minimize the likelihood and thus the consequences of any data breach—regardless of where it occurs in the supply chain. For public companies, the consequences can be far-reaching: In the United States, the Securities and Exchange Commission's guidance requires that companies not only disclose material cyber security events when they occur, but also disclose material risks that could occur. For those companies that outsource functions with material risks, the guidance requires a description of those functions and how companies address the risks. But there is an upside to sound cyber security as well: Companies that truly embrace appropriately balanced cyber security measures could build capabilities that likely give them a considerable edge over their competitors.

The two Achilles heels of the supply chain

Any supply chain has both internal and external cyber vulnerabilities. This article is focused on the latter, but for context, it's worthwhile to look briefly at the internal issues.

Within the four walls of the organization, systems are becoming markedly more vulnerable to cyber attacks. This is especially true in the manufacturing industry, where industrial control systems (ICSs), based on proprietary technology, have historically controlled automated production processes. Those systems were isolated from the network, meaning that to use them, factory operators had to be physically present and know how to use them.

However, over time, ICS systems (such as SCADA,

for example) began using "standard" technology (such as the Windows operating system, or SQL server as a database) and are now connected to the corporate network so they can consolidate and share information across the enterprise. This provides significant added value in that it enables companies to monitor and manage production remotely, but it also increases the chance of being subject to a cyber attack.

Additionally, there are now more ways to access industrial control systems. Once they are more broadly networked, physical access is no longer required. The system might then be accessed by malware spread across the corporate network. The malware no longer needs to be custom written for proprietary operating systems because the new systems are based on common commercial platforms. Now, a simple malware infection on a corporate IT system can easily spread to the industrial system if not properly protected.

When you move outside the four walls of the organization, the problem is just as worrisome. Most companies now manage hundreds and sometimes thousands of external, outside vendor relationships, most of which involve some level of information sharing and access. This creates significant vulnerabilities, especially when these processes are automated. Gone are the days of fortification when a company could build a firewall around its IT perimeter and protect its information; most companies can no longer even draw a distinct line around their network perimeters, so fuzzy are the boundaries between their networks and those of their partners. Vendor integration, along with the adoption of Cloud-based computing services and employee programs such as bring-your-own-device (BYOD) and telecommuting, have nearly eliminated the corporate perimeter entirely.

Some companies are now struggling to find ways to manage and govern this problem, which is not just an IT or procurement issue. It's a corporate-wide risk issue, which now is getting the attention of legal and compliance groups. What, then, is needed? The answer is the development of more sophisticated oversight programs.

Dampening external supply chain risks

So what will it take to do that—and thus to mitigate cyber security risk in the supply chain? These days, there is no shortage of good information available to describe responses to cyber security in general. But the authors of this article have found that the following approaches are especially relevant for guarding against breaches of the external supply chain.

- **Map the data flows in the supply chain.** Most business

leaders now recognize that data is a primary asset, but fewer have a clear understanding of how data flows in and out of their companies, who they are sharing it with and how those flows are being managed and controlled—both internally and externally.

• **Plan a comprehensive risk assessment.** The organization's approach to cyber security should not be viewed in isolation from its mainstream business activities; they are too tightly interconnected. The level of protection has to be proportional to the potential impacts and likelihood of an incident. For this reason, an information security risk assessment could be the right way to assess the security of the supply chain and identify the critical areas to be addressed. The assessment will go beyond the data mapping noted above. Ideally, a third party whose independence can help ensure objectivity should conduct the assessment.

• **Align with emerging standards.** New standards have been developed as companies become aware of cyber security risks, especially with regard to the supply chain. In particular, organizations such as the Nation Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO) have published frameworks and guidelines related to the management of cyber security. These frameworks, created through collaboration between government and the private sector, use a common language to address and manage cyber security risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses. NIST has also produced a short animated video* about the framework that is intended for C-suite executives as well as cyber security professionals.

Many other organizations and standards-setting communities have followed suit with their own frameworks. One of the most important features of these frameworks is their emphasis on the importance of the capabilities needed to respond to cyber attacks. The understanding is that attacks are inevitable, so rather than just seeking to guard against them, it is crucial to build systems with the resilience to rapidly respond and ideally to minimize the damage they can cause.

• **Set clear expectations in all supply chain contracts.** Admittedly, this is easier said than done. Yes, contractual clauses around security levels and assurances are a necessary step, but many companies are struggling to define the levels of specificity required in such clauses, and wrestling with the issues of cyber security audits and enforcement monitoring. When you have thousands of suppliers, how can you possibly audit all of their security controls? It's hard enough to audit your own. Third-party certifications and attestations are helping, but there are still plenty of gray areas about the scope of the attestation and how effective they are. Certifications are also expensive and time-consuming for vendors to achieve, and it's difficult to define the level and type of certifications they need.

Furthermore, not all certifications are equal, and companies must be alert to clever marketing by suppliers boasting of certifications for new data centers, for instance. Customers must look closely to ensure that it is the vendor's own controls that are being certified—not just that the vendor is using a third-party data center that is certified.

Supply chain connections range from the exchange of purchase order details via e-mail or other electronic exchange, to vendor-controlled facility management systems, to integrated design and production environments—all of which are potential security vulnerabilities.

Simplicity is the safest approach: Organizations should ensure that all of their outsourcing contracts require their suppliers to adhere to defined maturity and audit standards; that they do this in turn with their suppliers; and that they agree to provide access to cyber security audit results at least once a year. If a supplier cannot show such results and is reluctant to agree to such practices, then perhaps their vendor status should be reconsidered.

• **Insure, but never depend on it.** Certainly, insurance coverage can help to shift the risk, but we are now seeing that it's often not enough to cover losses. For example, Home Depot, whose massive breach made headlines around the world a few years ago, is now up to hundreds of millions of dollars in costs and still has dozens of lawsuits pending. The cap for most insurance policies designed to cover damages from cyber security breaches is usually

about $100 million, and many such policies have a myriad of gaps in their coverage. Moreover, coverage may be denied or limited where companies do not diligently assess and manage their data-sharing relationships. The patchwork of regulatory frameworks around security requirements, data privacy, and cross-border data transfer and data localization laws only serve to compound the problem and make governance more complex.

There is an upside to sound cyber security as well: Companies that truly embrace appropriately balanced cyber security measures could build capabilities that likely give them a considerable edge over their competitors.

How suppliers should handle customer information

And what obligations do suppliers have? What should be their priorities when it comes to recognizing their roles and responsibilities in guarding supply chains against cyber attacks—and building more resiliencies into their systems when cyber criminals do break in?

As a fundamental, a supplier should understand the security protections they should be offering to protect their customers' data. A prerequisite, of course, is that they acknowledge and assess the connectivity between them, and thus have a clear idea of the risks that they, as the supplier, may be introducing as a consequence of their handling of supply chain data.

At the same time, suppliers should strive for compliance with recognized security certifications. The most common among these include the U.S. Health Insurance Portability and Accountability Act (HIPAA) assessments, the American Institute of Certified Public Accountants Service Organization Control Reports (SOC 2) and the Payment Card Industry Data Security Standard (PCI-DSS). As a recommendation, suppliers should be aligned with the ISO 27001:2013 standard—the internationally applicable Information Security Management System. However, compliance with those certifications is unlikely to be enough; suppliers must seek out and work to comply with certifications specific to their industries and to their customers' needs.

Moreover, suppliers must help prevent supplier fraud—a growing problem these days, even though it doesn't require technical expertise by the perpetrators. Their customers stand to lose a lot if the procurement or finance team is duped by a legitimate-looking e-mail from a supplier asking to change the banking details for a big payment. To minimize the likelihood of unwittingly enabling such scams, suppliers should proactively work to establish better lines of communication with their customers—for example, agreeing on a process that includes additional steps for further confirmation of any such change to their banking details.

What opportunities can cyber security create?

So far, we have emphasized protection against the downside of cyber security breaches. But there is a more positive perspective too: the idea that high levels of supply chain data security can be used for competitive advantage. For example, promotes its ISO 27001 certification for Online Banking and Mobile Banking services on its Website.**

More and more customers can be expected to look for demonstrably high levels of security. Suppliers that can show bona fide security framework certifications such as ISO 27001 could conceivably expect to be able to factor those credentials into their pricing and future contract negotiations. Furthermore, proven cyber security credentials can be used to establish differentiation—to show that one's company is more secure than others in its markets.

Clearly, the topic of supply chain cyber security is timely and fraught with challenges all its own. There are far more subtleties and interpretations to describe than can be laid out in a single article. But if there is one message that the authors hope to convey, it is that the issue is not one that can be postponed until the next meeting of the board of directors—or worse, until the next security breach. British wartime leader Winston Churchill was famous for his insistence on "action this day." We think that is an appropriate maxim for tackling the many cyber security onslaughts of the 21st century.

* The NIST video can be viewed at nist.gov/cyberframework
** Barclay's online certification can be viewed at barclays.co.uk/Security/ISO27001certification/P1242561780370