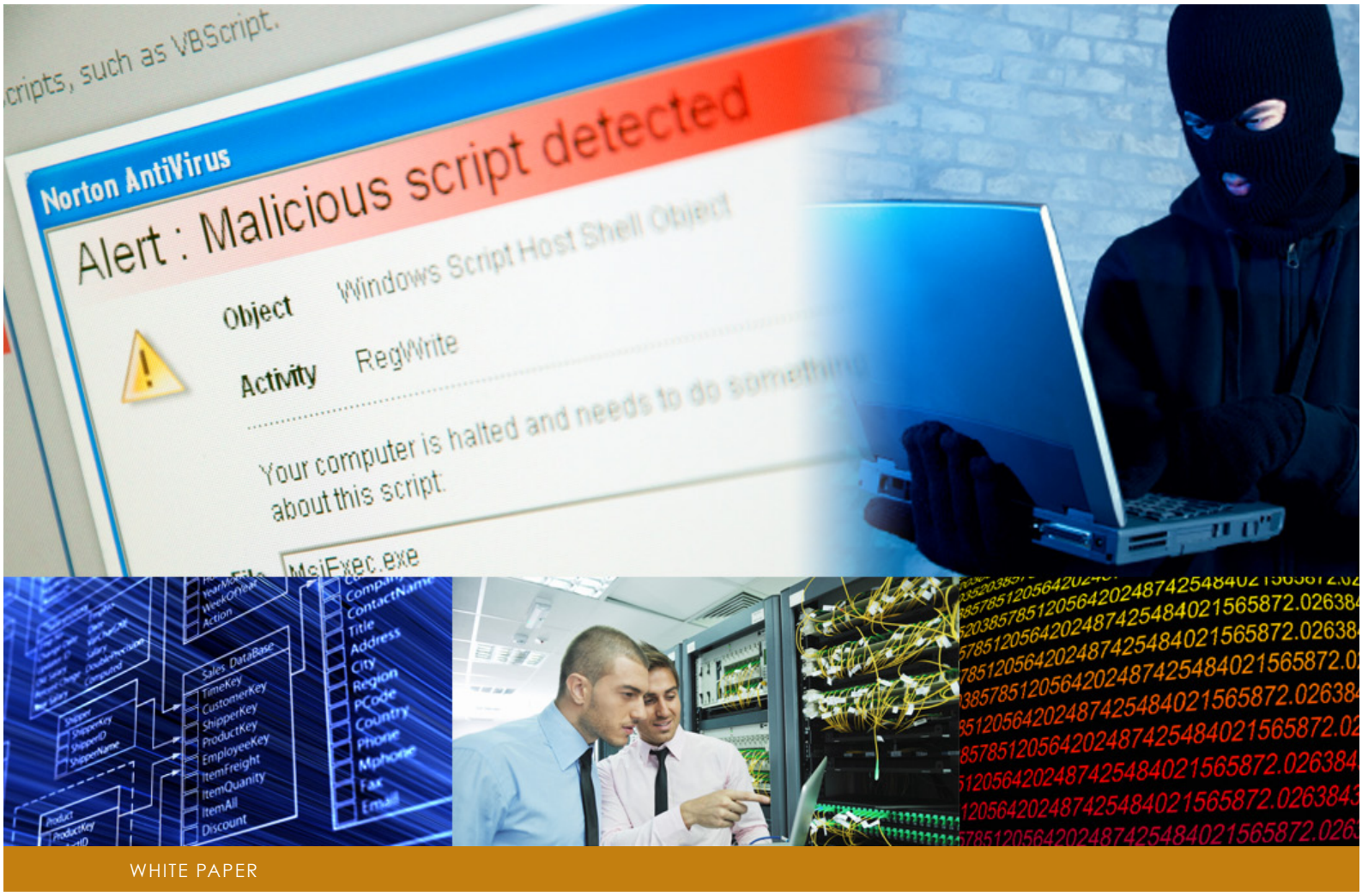

WHITE PAPER

Managing Cyber Supply Chain Risks

May 2013

Sponsored by:

OneBeacon
PROFESSIONAL INSURANCE®

Managing Cyber Supply Chain Risks

Executive Summary

Supply chain risks often are characterized in terms of tangible property exposures such as fires and natural catastrophes. Physical damage to buildings, machinery and transportation infrastructure, however, are not the only potential causes of supply chain disruptions. Information and communication technologies are vulnerable to hardware and software failures, as well as to damage caused by hackers and malware writers. Significant cyber-related supply chain disruptions are rare, but a large-scale cyber event holds the potential to be as damaging as a major natural catastrophe. Companies should implement a supply chain risk management program to proactively address these exposures. They also should consider insurance specifically designed for cyber-related risks, including supply chain risks.

Introduction

Cyberspace has long been plagued by hackers and malware. Hackers can trace their origins to the "phone phreaks" of the 1970s, who hacked into phone systems to make free long distance calls.[1] The first virus was set loose on the Internet even before it was the Internet: the Creeper virus was first detected on ARPANET, the forerunner of the Internet, in 1971.[2] Early on, hackers and virus writers were more annoying than dangerous, but today they represent serious threats not only to individuals and businesses, but to entire nations and even the global economy.

According to Norton, the global cybercrime industry – which is now dominated by organized, professional gangs – has already overtaken the global trade in heroin, cocaine and marijuana.[3] Politically motivated hackers – "hacktivists" – have penetrated heavily fortified military and government intelligence networks. China has been implicated in systematic attacks on U.S. computer networks – from the Defense Department to Google to JP Morgan Chase. A 2008 Russian cyber assault crippled the essential electronic infrastructure of the Republic of Estonia.

Security experts say that businesses are not doing enough to protect themselves from increasingly dangerous cyber threats. Some are concerned that even the best security is not good enough. Dell Inc's chief security officer, John McClurg, interviewed by The Fiscal Times, frets that the bad guys "outspend us and ... outman us in almost every way."[4] Cyber security authority Richard Clarke, speaking to the U.S. Naval Academy, lamented that "American companies cannot successfully protect their networks against the Chinese People's Liberation Army. The big companies that really should know this stuff - the ones that are spending millions of dollars defending their networks such as Google, Sony, City Bank, Bank of America - they all have been successfully penetrated."[5]

In a world where even the most sophisticated networks are vulnerable, corporate decision makers should be concerned about not only their own system defenses, but also those of their customers, suppliers and other business partners. Supply chain risk management is a topic that has received a lot of attention recently, but typically in the context of natural disasters such as the Tohoku earthquake and tsunami and the Thailand floods in 2011. Supply chains also are vulnerable to disruptions from cyber-related events. A single supplier that is temporarily shut down as the result of an internal systems problem could be a major headache to its customers. An entire business sector brought to its knees by a cyber blitzkrieg could result in massive supply chain disruptions that reverberate through the world economy.

Supply chain vulnerabilities

Disruptions could be a result of a software or hardware malfunction within a supplier's own system, or they could be caused by an external attack.

The devastating 9.0 magnitude earthquake that struck off the coast of northeastern Japan in March, 2011, along with the ensuing tsunami, damaged transportation infrastructure and crippled factories that supply everything from auto parts to steel. Several months later, Thailand was overwhelmed by the worst floods in half a century, shutting down more than 14,000 businesses. More recently, and closer to home, Superstorm Sandy closed shipping terminals, submerged warehouses, and left thousands of businesses without power.

Manufacturers, wholesalers and retailers around the world were impacted when key suppliers were knocked out of business – some permanently – by these events. Even suppliers that were able to continue manufacturing often were not able to ship their goods because of damaged roadways and ports. The computer and automobile industries were particularly hard hit.

These and other recent events have highlighted the fact that a far-flung network of suppliers can increase vulnerability to supply chain disruptions. This is especially the case for businesses employing "just in time" or "just enough" inventory strategies, for which even a short-term disruption can have highly negative consequences. In the aftermath of these catastrophes, many companies are reassessing how they manage their supply chains and are taking steps to minimize the impact of disruptions.

Of course, natural catastrophes are not the only cause of supply chain disruptions. Potential sources of large-scale disruptions include war, political instability, labor disputes and economic recession. Sometimes much smaller scale events can be highly significant: damage to even a single facility can have disastrous consequences. An explosion at the Evonik factory in Germany, for example, affected half of the worldwide supply of CDT, a resin essential to auto parts manufacturers.[6] From the perspective of an individual company, the loss of any hard-to-replace supplier for any reason is a critical event.

Increasingly, disruptions caused by problems with websites and computer networks are recognized as a significant supply chain threat. Disruptions could be a result of a software or hardware malfunction within a supplier's own system, or they could be caused by an external attack. An attack in the "cloud" – where a vendor that provides services to thousands or even millions of companies may be targeted – could cause widespread disruptions across many industry sectors. In an extreme, but increasingly probable scenario, massive disruptions could result from a large-scale attack on the infrastructure of an entire nation.

"Supply chain" typically implies the movement of physical items, but in a world where digital assets often exceed the value of physical assets, the concept of supply chain needs to be expanded to include information and services. Organizations of all types rely on the Internet and various software tools and service providers to order and pay for supplies, to trade information with business partners and to transact business with customers. Interruption of those processes, even for companies dealing in the bricks-and-mortar world, potentially can be even more disruptive than damage to transportation infrastructure. Companies, such as Advisen Ltd., whose products are largely digital can be crippled if their information suppliers or digital infrastructure vendors are unable to perform.

The business impact of cyber events

These attacks may originate with cyber criminals looking to gain access to valuable information; hacktivists or terrorist groups seeking to damage companies they view as violating political, religious or cultural beliefs; or nation states engaging in cyber espionage or even cyber sabotage.

Almost every company experiences problems due to software or hardware malfunctions. Typically these events are little more than inconveniences, though on occasion computer problems can be devastating. An Australian t-shirt company that distributed its products through Amazon.com was sunk by three lines of code designed to automatically generate slogans from electronic dictionaries and verb lists. Unbeknownst to the company until it was too late, Amazon was advertising t-shirts with messages such as "Keep Calm and Grope On" and "Keep Calm and Choke Her."[7]

The more common scenario is a company impaired in its ability to do business by a computer-related failure. In what was at first reported to be an attack by hactivist collective Anonymous, web host GoDaddy was shut down for six hours in September, 2012 by "a series of internal network events that corrupted router data tables."[8] Go Daddy claims to be the world's largest hosting provider of secure websites with more than 53 million registered domain names. The outage affected not only GoDaddy itself, but also the many companies that conduct business through its web hosting services.

Of growing concern to companies are malicious attacks against websites and networks. These attacks may originate with cyber criminals looking to gain access to valuable information; hacktivists or terrorist groups seeking to damage companies they view as violating political, religious or cultural beliefs; or nation states engaging in cyber espionage or even cyber sabotage. Falling victim to such events can make a company an unattractive business partner, compromise its ability to conduct business, or even force it to shutter its doors. Consider the following examples:

- DigiNotar, a Dutch company that issued digital certificates that authenticated online transactions, was forced out of business after a security breach resulted in the issuing of fraudulent certificates.
- A large U.S. metropolitan utility suffered a massive "distributed denial of service" (DDoS) attack, which knocked out its automated online- and telephone-payment systems for 48 hours.[9]
- A U.S. power plant was taken off line for three weeks when a computer virus attacked a turbine control system. The virus was introduced when a technician unknowingly inserted an infected USB computer drive into the network.[10]
- In what is regarded as among the most destructive acts of computer sabotage on a company to date, a virus erased data on three-quarters of the corporate PCs of oil giant. Saudi Aramco. United States intelligence officials claim Iran was behind the attack.[11]

Cyber-attacks typically target individual organizations or a well-defined group of organizations, but they have the potential to cripple a business sector, or even an entire country.

Cyber-attacks typically target individual organizations or a well-defined group of organizations, but they have the potential to cripple a business sector, or even an entire country. Government employed or sponsored hackers hold the potential for the most devastating attacks. Cyber warfare is no longer a threat – it is a reality. It is becoming a regular occurrence for countries to launch limited digital salvos at one another.

A recent cyber-attack caused computer networks at major South Korean banks and top TV broadcasters to crash simultaneously. North Korea is suspected of being behind the assault. A large scale cyber-attack could be directed at a country's digital infrastructure, as was the case of the Russian attack on Estonia in 2008. Power grids, telecommunication networks and air traffic control systems all are potentially vulnerable. Of growing concern is an attack that cripples a country's physical assets, potentially causing widespread bodily injury and property damage. It is conceivable that a cyber-attack could result in airliners crashing or nuclear reactors melting down.

At the other end of the spectrum, owners and managers of small and midsize businesses often dismiss the threat of cyber-attacks. However, no company should assume it is too small to attract the attention of hackers. In fact, smaller businesses have become a favorite target of cyber criminals who view them as low risk/high reward targets. During the first six months of 2012, more than a third of targeted attacks on businesses were directed toward companies with fewer than 250 employees, according to security vendor Symantec.[12] Small and medium size businesses also should not assume that their only cyber exposure is from stealthy hackers secretly breaking into their systems. A small firm that processes credit card payments online, Card Solutions International, claimed to be a victim of cyber extortionists that reportedly shut down the company's website for a week after it refused to pay $10,000.[13]

Business interruption risks and risk management

Significant supply chain disruptions caused by cyber-related events, fortunately, are still uncommon. That should not be an excuse for complacency, however. The risks are very real. Disruptions can occur at any point on the chain. The following scenarios could occur at any time.

- A virus infecting the systems of a key supplier destroys essential records, forcing the supplier to shut down its systems for several days to eradicate the infection. Once the systems are back online, customers are required to resubmit their orders, causing further delays.
- A malicious attack on a trucking company disrupts its dispatch, freight management and logistic systems, resulting in delays in shipments of vital parts.
- A successful attack on a large commodities exchange interrupts the flow of essential materials and causes increased price volatility throughout numerous markets.

Supply chains are often understood in terms of manufacturing processes, but "supplies" also can be digital. A news publication, for example, may rely on a steady stream of content from newswires, freelance journalists and staff writers. A cyber event that disrupts the production or transmission of content could be highly damaging.

Companies also should consider insurance for their contingent business interruption exposures.

In addition to damage to suppliers and transporters, companies should be concerned about the digital infrastructure that supports modern commerce. Almost every business today relies on third parties such as internet service providers and web hosting services to support supply chain activities. Interruption of services provided through this digital infrastructure could be extremely disruptive – potentially even more disruptive in the short run than damage to physical infrastructure caused by a natural catastrophe.

The risk of supply chain disruptions caused by system malfunctions, hackers or viruses should be managed much the same as other supply chain risks. Supplier diversification is essential – relying on a single supplier is simply asking for trouble. Additionally, the quality of cyber defenses should be a criterion when evaluating potential suppliers. For critical suppliers, a system security audit may be justified.

Companies also should consider insurance for their contingent business interruption exposures. First party cyber insurance policies may provide coverage for extra expense, business interruption, and contingent business interruption losses due to a cyber-attack. Organizations should work with their brokers to assure that their insurance programs provide the coverage appropriate to their supply chain exposures.

Conclusion

Security experts warn companies that it no longer is a matter of "if," but rather a matter of "when," or even "how often," their systems will be attacked. A serious data breach can cost a company millions of dollars in remediation, notification and mitigation costs. Most breaches, however, do not cripple a company's ability to conduct business. In fact, sophisticated hackers make it a point to not interfere with a company's operations so that they can continue to siphon valuable information from its systems.

On the other hand, some attacks can bring a company to its knees. In a growing number of cases, the objective of an attack is specifically to damage an organization. This is especially true for attacks by hacktivists and cyber terrorists. Waves of attacks in 2012 and 2013 targeting U.S. financial institutions by the Izz ad-Din al-Qassam group, for example, are part of a larger trend of disruptive and destructive attacks on financial institutions by groups motivated by political, social or religious causes. These sorts of malicious attacks have the potential for causing significant supply chain disruptions.

Of course, bad guys are not the only source of computer-related problems. Hardware and software failures can hobble a company, potentially causing significant issues for suppliers, customers and other business partners. Whatever the source of a failure, however, companies should be aware of the potential for supply chain disruptions, and take proactive steps to manage the risks. One effective tool for offsetting the financial impact of a supply chain disruption is insurance. Many cyber insurance policies now provide contingent business interruption coverage for losses due to various types of events. Insurance buyers should consult with a broker with extensive knowledge of cyber risks and cyber insurance coverages to assemble an insurance program that addresses the full range of their cyber exposures, including supply chain risks.

NOTES:

1 "A history of hacking," St. Petersburg Times http://www.sptimes.com/Hackers/history.hacking.html

2 "40th anniversary of the computer virus," Help Net Security http://www.net-security.org/malware_news.php?id=1668

3 "The terrifying rise of cyber crime: Your computer is currently being targeted by criminal gangs looking to harvest your personal details and steal your money," Mail Online http://www.dailymail.co.uk/home/moslive/article-2260221/Cyber-crime-Your-currently-targeted-criminal-gangs-looking-steal-money.html

4 Hackers Are Multiplying and Targeting the U.S." The Fiscal Times http://www.thefiscaltimes.com/Articles/2013/02/25/Hackers-Are-Multiplying-and-Targeting-the-US.aspx#17G47VT3MgsqQQdM.99

5 "Cyber Security Expert Discusses U.S. Vulnerabilities at Naval Academy," America's Navy http://www.navy.mil/submit/display.asp?story_id=72290

6 "How An Explosion In Germany Could Disrupt The Global Auto Supply Chain For Months," Business Insider http://www.businessinsider.com/morgan-stanley-explosion-germany-disrupt-global-auto-supply-2012-4#ixzz29AxYdA8q

7 "Computer error" sinks online T-shirt business," TechEYE.net http://news.techeye.net/internet/computer-error-sinks-online-t-shirt-business

8 "GoDaddy Outage: Anonymous Attack Or IT Failure?" InformationWeek http://www.informationweek.com/security/attacks/godaddy-outage-anonymous-attack-or-it-fa/240007167

9 "Organized Crime Hackers Are The True Threat To American Infrastructure," The Economist (reprinted in The Business Insider) http://www.businessinsider.com/organized-crime-hackers-are-the-true-threat-to-american-infrastructure-2013

10 "UPDATE 1-Malicious virus shuttered U.S. power plant -DHS," Reuters http://www.reuters.com/article/2013/01/16/cybersecurity-powerplants-idUSL1E9CGF-PY20130116

11 "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," The New York Times http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all&_r=0

12 "Hackers increasingly zero in on small businesses, Symantec says" http://www.csoonline.com/article/712942/hackers-increasingly-zero-in-on-small-businesses-symantec-says

13 "FBI Investigating Cyber-extortion," InfoSecNews.org http://www.infosecnews.org/hypermail/0405/8594.html