DAMBALLA

WHITEPAPER

Corporate Risk and Due Diligence in the Cyber Threat Crosshairs

WHY THE C-SUITE MUST LEAD

Imagine walking into the office tomorrow morning and finding your most critical corporate secrets have suddenly become public domain. Financial information, confidential communication, technical blueprints, everything. Will it flood the market with cheap clones of your most valuable products? Will it derail sensitive business operations, relationships or revenue? Worse, what if critical production processes have been quietly sabotaged, triggering anything from quality problems to environmental disasters and loss of life?

While these scenarios may appear extreme, cyber risks have rapidly developed into a major threat for global economies and enterprises. With little notice, cyber threats have reshaped corporate risk profiles and have transformed cyber security from a back-office concern into a foreground corporate priority. Corporate boards and auditors are increasingly zeroing in on cyber risk,[1] due to its potential to enhance or destroy financial forecasts, valuation, reputation, compliance and more.

Fortunately, new solutions can help the C-suite protect balance sheets, reputation and valuation in an increasingly toxic cyber environment.

"We are in a constant state of seeing activity against critical infrastructure"

—Greg Schaffer, U.S. Department of Homeland Security Assistant Secretary for Cyber Security and Communications

New IT Environment, New IT Risks

For many years, information technology (IT) played a supporting role in the executive suite and boardroom. Today, IT has transformed into an enabler of business strategy and advantage, often through the use of innovative social network, mobile and cloud technologies.

As valuable as these new opportunities are, they incur enterprise risk that must be measured and managed. Traditionally, finance and risk officers focus on protecting key metrics such as return on invested capital, output, profits and valuation. When they build their risk management radar, they track any strategic, financial, operational or safety risk that could jeopardize the company's metrics.

IT security has rarely been on that radar. From the executive suite, information security systems like firewalls, antivirus, and intrusion prevention could feel a little like plumbing – important, but easy to procrastinate over – until there was a leak.

Things are leaking now. Cyber threats now pose a targeted threat to critical operations and assets. At the macro level, the World Economic Forum ranks cyber security among five top "risks to watch," due to their "potential for severe, unexpected or underappreciated consequences." The WEF, in collaboration with partners such as Marsh & MacLennan Companies, the Wharton Center for Risk Management and Zürich Financial Services, placed cyber risk alongside global resource insecurity, resistance to globalization, weapons of mass destruction and social instability in emerging economies.[2] Dense interconnectivity means cyber theft, data fraud, digital misinformation, terrorism and infrastructure neglect could potentially trigger critical systems failures and major systemic financial failure.[3]

Unfortunately, enterprises are along for the ride, like it or not. For them, the current cyber environment is increasingly hostile and shows no respect for corporate budget cycles. The past two years spawned more than 2 million viruses, worms, backdoors and Trojans. In parallel, loud, clumsy hackers were replaced by sophisticated stealth attacks and industrial espionage sponsored by crime rings, companies and nation-states.[4]

The potential exposure of this shift is mounting quickly. In 2011, surveyed U.S.-based multinationals experienced more than one successful cyber attack per week, up 45% from 2010.[5] 2011 also saw the U.S. Computer Emergency Readiness Team (CERT) respond to more than 100,000 incident reports and release more than 5000 actionable security alerts.[6] These attacks brought the potential for catastrophic loss and the problem is only going to get worse. As framed by the hacker group Anonymous, "Expect Us."

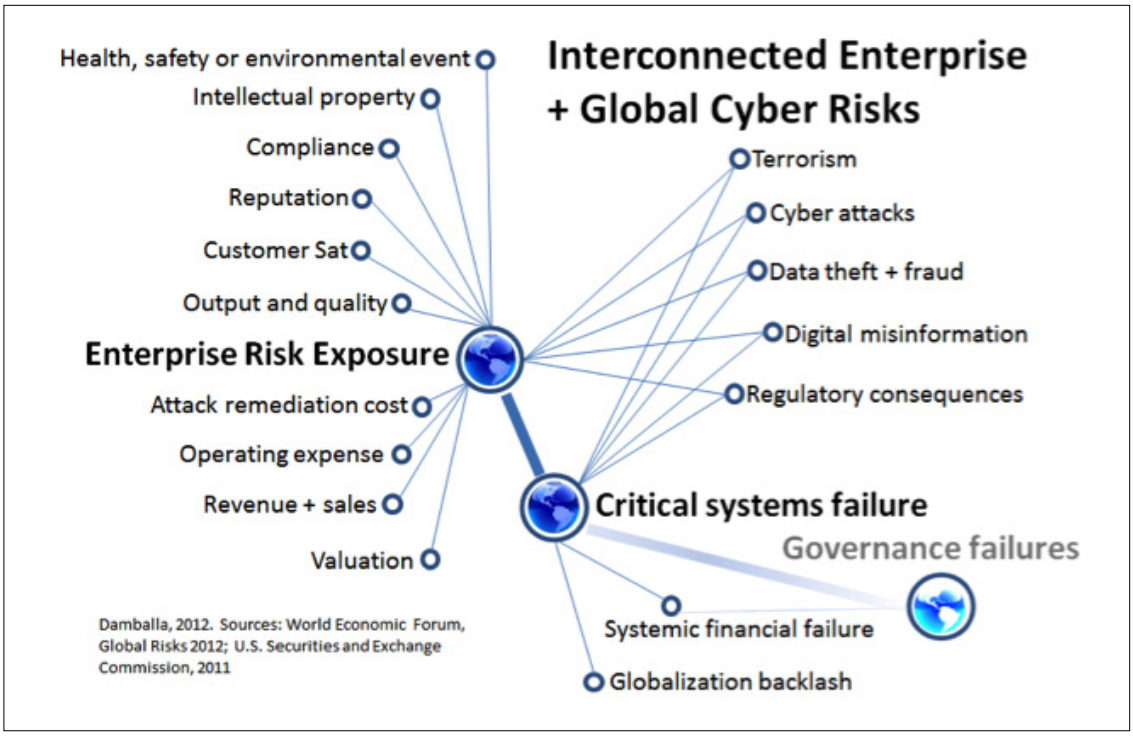

Figure 1: Interconnected Enterprise + Global Cyber Risks

> "It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently."
>
> —Warren Buffett

What's the Exposure?

For corporations, a cyber attack means more than just sending spam to everyone in your address book. It's also not something easily cured by an insurance claim. Cybercrime can incur crippling intangible costs, ranging from public reputation and investor confidence to stock valuation and business integrity.

IT'S NOT JUST A BANK AND MERCHANT PROBLEM

Firms that handle money are obvious targets, but cybercrime also directly threatens facilities in energy, manufacturing, refining, transportation, energy, government and other sectors. While each enterprise has unique risks, virtually every type of crucial asset has been successfully attacked in recent history. Examples include sensitive data, intellectual property and financial systems.[7] [8] [9] [10] [11] [12] [13] [14] Cyber threats can even jeopardize physical assets, environmental safety and human lives, as exemplified by attacks on military weapon systems (U.S. Air Force) industrial control systems, public water and sanitation, transportation, and power plants.[15] [16] [17] Vulnerabilities have already been exploited or identified in SCADA industrial control software from Siemens, General Electric, Rockwell Automation, Koyo Electronics and other vendors.[18]

Depending on the attack severity and duration, a successful exploit can draw liability and scrutiny as well as undermine compliance, revenue, investor confidence and valuation. Cyber attacks or espionage directed at critical intellectual property or classified data can also destroy competitive capabilities or even business integrity. Of course, attacks directed at critical infrastructure can trigger widespread shutdowns, environmental disaster or loss of life. Already, attacks have derailed trains, commandeered military drone aircraft and tampered with nuclear system controls.[19] [20] [21]

Cyber attacks also incur tangible direct costs that can wipe out millions in potential profit. Examples include lost revenue, litigation and damages and liability associated with data loss, and environmental damage or loss of life. Cybercrime also incurs direct costs for attack remediation, customer service and other incremental operating expenses. A benchmark study of U.S. Companies found the direct costs of cybercrime ranged from $1.5 to $36.5 million each year, with the median annualized cost of $5.9 million.[22] In addition, costs rise quickly if the intrusion is not addressed quickly. On average, it takes an enterprise 18 days to resolve the cyber attack, with an average cost of $416,000 per incident. At $23,000 per day, an undetected track or prolonged resolution substantially increases remediation costs and may amplify the potential for catastrophic damage. Obviously, an attack that involves environmental damage or loss of life would be substantially more costly.

Cybercrime is not just a problem for banks and merchants. It directly threatens facilities in energy, manufacturing, refining, transportation, energy, government and other sectors.

While an enterprise may not be able to alter the global cyber threat, it does have control over its own risk profile.

The Enterprise Problem

While an enterprise may not be able to alter the global cyber threat, it does have control over its own risk profile. To accomplish this, there are three initial issues to accept.[23]

LEGACY CYBER DEFENSES FALL SHORT

In a Hollywood caper movie, bad guys don't wear name tags and don't drive a vehicle with "getaway car" painted on the side. Instead, they tunnel through walls, use disguises, disconnect surveillance cameras and evade the security guard's route. Modern cyber criminals are no different. They expect enterprise networks will be defended by firewalls, antivirus, passwords, behavioral anomaly triggers and other obstacles. They've learned how to work around them.[24] Also, modern cyber attacks rarely show the same face twice; roughly 100 unique malware files and 800 new malicious URLs are posted hourly (80% of these appear on legitimate, but compromised, websites).[25] As a result, attack signatures and site blacklist "mug shots" are obsolete the day they are posted.

SOCIAL MEDIA, MOBILE, GLOBAL PRESENCE, "BYOD" AND THE CLOUD AMPLIFY THE PROBLEM

Social networks and mobile technology are valuable enterprise tools because they make it easy to communicate anything, from anywhere, with anyone. Unfortunately, cyber criminals hijack and invert these capabilities to penetrate enterprise networks.[26] Social networks facilitate pre-attack reconnaissance and make it relatively easy to impersonate employees and distribute malware.[27] Also, a diverse array of corporate and employee-owned user accounts, laptops and mobile devices make it impractical to define the network perimeter or enforce reliable endpoint controls. Global presence and the cloud can aggravate this, by exposing sensitive corporate assets to diverse hosting, governance, employment, intellectual property and law enforcement models.[28] [29]

Alternative Response Strategies

While social networks, mobile devices and the cloud can create risk, they also drive innovation and advantage. As a result, a "kill the messenger" ban against them isn't attractive or practical – it would be like ripping out the phones to avoid telemarketers. Given the potential benefits, it makes much more sense to simply mitigate the risks. Unfortunately, while legacy network security tools are valuable against conventional threats, they are outrun and outgunned by the new challenges.

In theory, one possible response is to simply ignore the problem and hope it goes away. However, advanced malware is expected to be a top threat for many years.[30] Eventually something will happen, losses will occur and questions will be asked. Any case for delay will be forgotten and the resulting inaction and missed warning signs may look like negligence. A credible and proactive approach offers the best opportunity to avert serious problems.

So if old tools don't work and doing nothing isn't an option, what does work?

Addressing the Cyber Risk Challenge

While it's not possible to completely prevent cybercrime, there are solutions that offer a faster, cleaner and less painful recovery. Implemented properly, this can efficiently contain problems before they jeopardize corporate results, cause liability or create unwanted scrutiny.

Nearly 90% of data theft victims had evidence in their log files but failed to identify it. Fixing this is a great place to start. Tools that help your team quickly spot attacks can make the difference between a minor breach and worst-case scenario.[31] These systems also save money – on average, they cut breach costs by 24%, or about $1 million.[32]

Detecting a sophisticated cyber breach is rarely easy, but it's not impossible. Although cyber attack strategies are diverse and dynamic, they have common denominators. A master thief or spy needs a secret lair and a way to move stolen materials. Advanced cyber criminals are no different; eventually, they connect to an Internet-based command-and-control server for instructions or data transfer.

Even so, spotting advanced cybercrime while it's still a juvenile delinquent demands exceptional detective work. It requires the ability to continuously interpret massive amounts of data, discard irrelevant facts and see a coherent crime scene. Technically, it involves three dynamically correlated malware detection strategies:

1. Source and reputation monitoring,
2. Payload inspection, and
3. Network Visibility and Behavior Monitoring.

These processes continuously profile the who/where/when/what/why/how attributes of network users, data and traffic in context with each other and external criteria. In this approach, individual attributes may be good or bad; a jury of multiple factors makes the final determination.

The resulting 3-D contextual awareness is an effective countermeasure against advanced cyber threats, but it requires 24-7 inspection and correlation of network logs, packet content and activity. This vastly exceeds human abilities, but automated analysis and alert systems offer the same benefits with a much better return on investment. By offloading labor-intensive patrol duties, these systems focus high-value security talent as an efficient fast response team for trouble anywhere in the organization. They also ensure consistent surveillance and security controls across multiple facilities.

> "…A major cyber attack could potentially wipe out whole companies… cause serious damage…even kill people. While it may sound alarmist, the threat is incredibly real."
>
> —John Henry, FBI Executive Assistant Director

Seven Reasons Why Cyber Security Is a C-Suite Problem

In the past, cyber security may have only received grudging attention in the executive suite because it was seen as an IT help desk issue, not a strategic priority.[33] Quite suddenly, cyber risk has jumped onto the table as a major threat to forecasts, reputations, valuation and business integrity. Cyber threats can no longer be dismissed as unpredictable "black swan" events – an attack that catches the C-suite off guard may raise due diligence concerns, both internally and externally.

While IT will ultimately carry out the fight, delegating cyber security entirely effectively cuts senior management out of potentially catastrophic decisions. Executive prioritization and support for cyber security controls risk exposure in six key areas:

1. Valuation and the Bottom Line
2. Critical Enterprise Assets and Operations
3. Reputation, Relationships and Trust
4. Safety, Compliance and Liability
5. Performance and Competitive Ability
6. Due Diligence and Disclosure Requirements

The server room may feel like a long way away from the stock exchange, but in the end, they're inseparable. More than 80% of S&P 500 corporate value is based on intangible assets exposed to cyber risk, such intellectual property, confidential data, reputation and relationships.[34] [35]

Cyber attacks have destroyed more than $1 trillion of intellectual property and confidential information value.[36] [37] They've also damaged physical assets, undermined output and compliance, disrupted revenue and destroyed the bottom line.

At a worst-case scenario, no company wants its IT assets to be a contributing factor in a terrorist attack, environmental disaster or loss of life, especially if unaddressed security flaws were a contributing factor. The resulting liabilities and intangible impact of guilt is too large to calculate.

Clearly, cyber security is not just an IT problem. Cyber attacks can cause irreparable harm, but we're not helpless. By prioritizing and supporting the appropriate initiatives, the executive suite can ensure cyber threats don't leave an indelible mark on the enterprise.

"We've spent over 12 years building our reputation, brand, and trust with our customers.

It's painful to see us take so many steps back due to a single incident."

—Tony Hsieh, CEO of the recently hacked Zappos.com. CNN, January 16, 2012

Damballa Solution

Damballa is the leading provider of security solutions that protect enterprise, ISP and telecommunication networks against advanced malware, persistent threats, and zero-day targeted attacks. Our unique approach rapidly identifies the command-and-control infrastructure used by criminal operators to exfiltrate data from assets and devices infected with malware. Our signatureless solutions improve security both inside and outside the network perimeter and stop threats traditional prevention solutions miss. Damballa identifies the severity and intent of these attacks even when the malware evades detection.

ADVANCED THREAT INTELLIGENCE

Damballa FirstAlert is the advanced cyber threat intelligence system that powers the Damballa Failsafe and Damballa CSP offerings. Damballa FirstAlert detects emerging threats long before the rest of the security industry has discovered and analyzed the related malware, and it is based on more than a half a decade of global DNS traffic monitoring and malware analysis, superior machine learning technology, eleven patents pending and backed by some of the world's leading authorities in cyber threats and criminal networks.

References

1 Wall Street Journal MarketWatch, "Audit Committee Members See 'IT Risk' Shortcomings, 'Lack of Innovation' Posing Threats to Companies: KPMG Survey," October 24, 2011

2 World Economic Forum Risk Response Network, "Global Risks 2011, Sixth Edition"

3 World Economic Forum, "Global Risks 2012, Seventh Edition"

4 World Economic Forum Risk Response Network, "Global Risks 2011, Securing Cyberspace"

5 Ponemon Institute, LLC, "Second Annual Cost of Cyber Crime Study, Benchmark Study of US Companies," August 2011

6 ABC News, "Loss of Life and Major Computer Attack, Warns Homeland Security," October 27, 2011

7 Escapistmagazine.com "Sony's Stock Taking a Beating Following PSN Hack," May 6, 2011

8 CNN, "Zappos Hacked, 24 Million Accounts Accessed," January 16, 2012

9 MSNBC, "T.J.Maxx Theft Believed Largest Hack Ever" March 30, 2007

10 Daily Mail, "Hackers Claim Break-In of US Senate Computers As CIA Chief Panetta Warns Cyber Attack Could Be Next Pearl Harbor," June 14, 2011

11 Huffington Post, "Symantec Hack Exposes Antivirus Source Code," January 06 2012

12 Fox News the "Lockheed Martin Hit by Unspecified Cyber Incident," May 28, 2011

13 Government Computer News, "Data Taken an IMF Hack 'Political Dynamite," June 14, 2011

14 BBC, "North Korea behind South Korean Bank Cyber Hack," May 3, 2011

15 ABC News, "Loss of Life and Major Computer Attack, Warns Homeland Security," October 27, 2011

16 CHEManager Europe, "Cyber Security for Industrial Control Systems," January 27, 2011

17 CHEManager Europe, "Cyber Security for Industrial Control Systems," January 27, 2011

18 Wired, "Hoping to Teach a Lesson, Researchers Release Exploits for Critical Infrastructure Software," January 19, 2012

19 Wired, "Computer Virus Hits US Drone Fleet," October 7, 2011

20 The Register, "Polish Teen Derails Tram after Hacking Train Network," January 11, 2008

21 Daily Mail, "How the World's First Cyber Super Weapon 'Designed by the CIA' Attacked Iran and Now Threatens the World," December 7, 2011

22 Ponemon Institute, LLC, "Second Annual Cost of Cyber Crime Study, Benchmark Study of US Companies," August, 2011

23 Forrester Research, Incorporated "Malware and Trojans and Bots, Oh My!" February 28, 2011

24 Forrester Research, Incorporated "Malware and Trojans and Bots, Oh My!" February 28, 2011

25 Computerweekly.com, "Malware Volumes Grow 60% in First Half of 2011, Says Sophos," August 2, 2011

26 Forrester Research, Incorporated "Malware and Trojans and Bots, Oh My!" February 28, 2011

27 http://www.informationweek.com/articles/231000723?cid=RSSfeed_IWK_Authors

28 World Economic Forum Risk Response Network, "Global Risks 2011, The Future of India's Cyberculture"

29 World Economic Forum Risk Response Network, "Global Risks 2011, The Future of India's Cyberculture"

30 Forrester Research, Incorporated "Malware and Trojans and Bots, Oh My!" February 28, 2011

31 Verizon RISK Team + United States Secret Service, "2010 Data Breach Investigations Report"

32 Ponemon Institute, LLC, "Second Annual Cost of Cyber Crime Study, Benchmark Study of US Companies," August 2011

33 Computerworld, "Top Execs Need to Be Involved in Cyber Security, Study Says," March 31, 2010

34 CNN, "Analysis: the Hidden Cost of Cyber Crime," June 7, 2011

35 Echo Research, "What Price Corporate Reputation?," June 14, 2011

36 CNN, "Analysis: the Hidden Cost of Cyber Crime," June 7, 2011

37 American National Standards Institute, "The Financial Management of Cyber Risk," 2010

30.119.1012

ABOUT DAMBALLA Damballa is a pioneer in the fight against cybercrime. Damballa provides the only network security solution that detects the remote control communication that criminals use to breach networks to steal corporate data and intellectual property, and conduct espionage or other fraudulent transactions. Patent-pending solutions from Damballa protect networks with any type of server or endpoint device including PCs, Macs, Unix, smartphones, mobile and embedded systems. Damballa customers include mid-size and large enterprises that represent every major market, telecommunications and Internet service providers, universities, and government agencies. Privately held, Damballa is headquartered in Atlanta, Georgia.