coresecurity
by HelpSystems

CORPORATE RISK AND DUE DILIGENCE IN THE *CYBER THREAT CROSSHAIRS*

WHY THE C-SUITE MUST LEAD

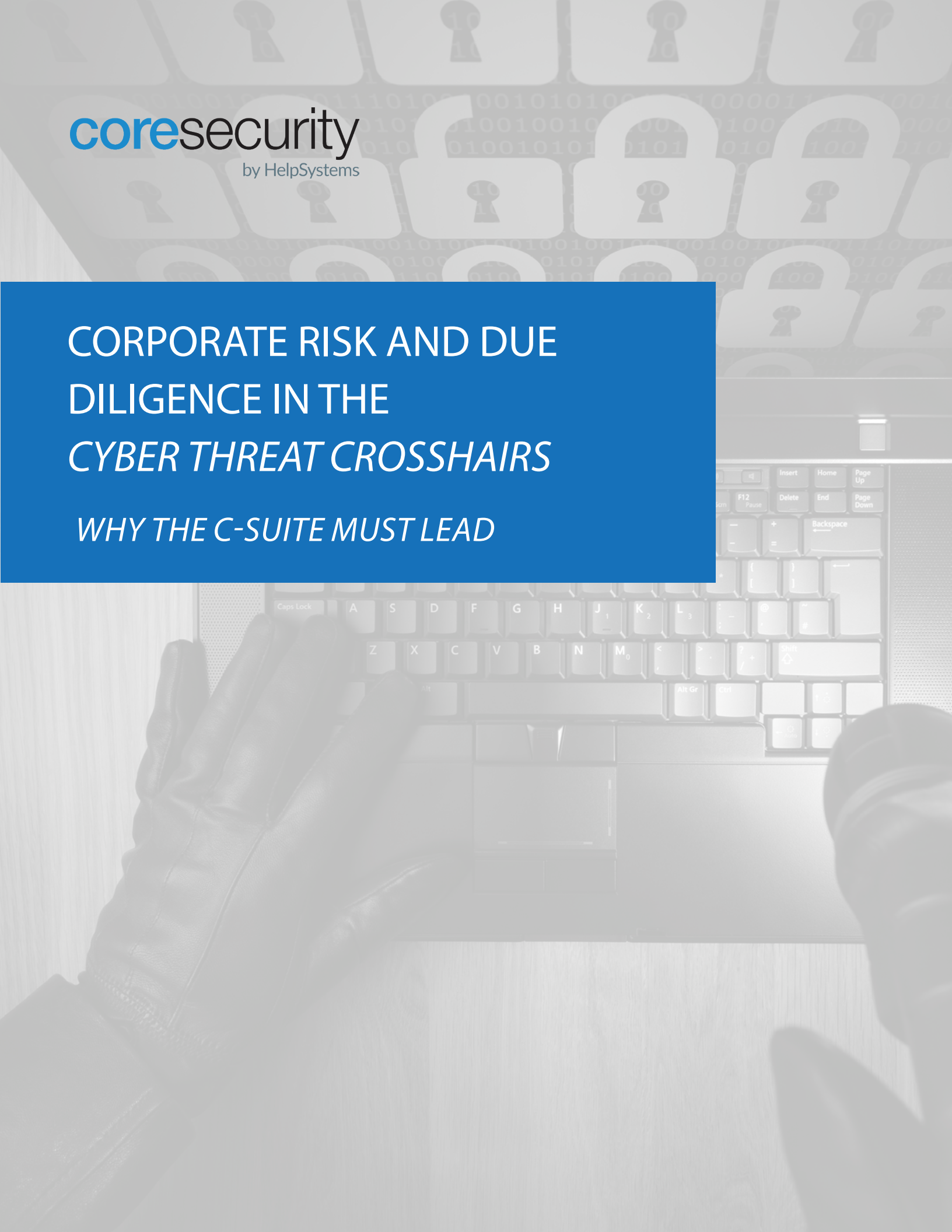


TABLE OF CONTENTS

INTRODUCTION

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 or 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 cybersecurity from a back-office concern into a foreground corporate priority.

Corporate boards and auditors are increasingly zeroing in on cyber risk because of 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.

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.

The past two years spawnedmore than two million viruses, worms, backdoors, and trojans.

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 cybersecurity among five top

www.coresecurity.com

'risks to watch' due to their 'potential for severe, unexpected or under-appreciated consequences.' In collaboration with partners such as Marsh & MacLennan Companies, the Wharton Center for Risk Management,

and Zürich Financial Services, cyber risk was placed alongside global resource insecurity, resistance to globalization, weapons of mass destruction, and social instability in emerging economies. Dense interconnectivity means cyber theft, data fraud, digital misinformation, terrorism, and infrastructure neglect could potentially trigger critical systems failures and major systemic financial failure.

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 two 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.

The potential exposure of this shift is mounting quickly. In 2011, surveyed U.S.-based multinationals experienced more than one successful cyberattack per week, up 45% from 2010. Also in 2011, the U.S. Computer Emergency Readiness Team (CERT) responded to more than 100,000 incident reports and released more than 5,000 actionable security alerts. 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.'

What's the Exposure?

For corporations, a cyberattack 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, 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. 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. Vulnerabilities have already been exploited or identified in SCADA industrial control software from Siemens, General Electric, Rockwell Automation, Koyo Electronics, and other vendors.

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. Cyberattacks 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.

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.

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. Also, modern cyberattacks 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). 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. Social networks facilitate pre-attack reconnaissance and make it relatively easy to impersonate employees and distribute malware.

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.

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. 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. These systems also save money, and on average, they cut breach costs by 24%, or about $1 million.

Improved Posture Against Critical Infrastructure Attacks

These processes continuously profile the who, where, when, what, why, and 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.

Tools that help your team quickly spot attacks can make the difference between a minor breach and worst-case scenario.

Detecting a sophisticated cyber breach is rarely easy, but it's not impossible. Although cyberattack 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:

- Source and Reputation Monitoring
- Payload Inspection
- Network Visibility and Behavior Monitoring

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.

Key Reasons Cybersecurity is a C-Suite Problem

In the past, cybersecurity may have only received grudging attention in the executive suite because it was seen as an IT helpdesk issue, not a strategic priority. 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.

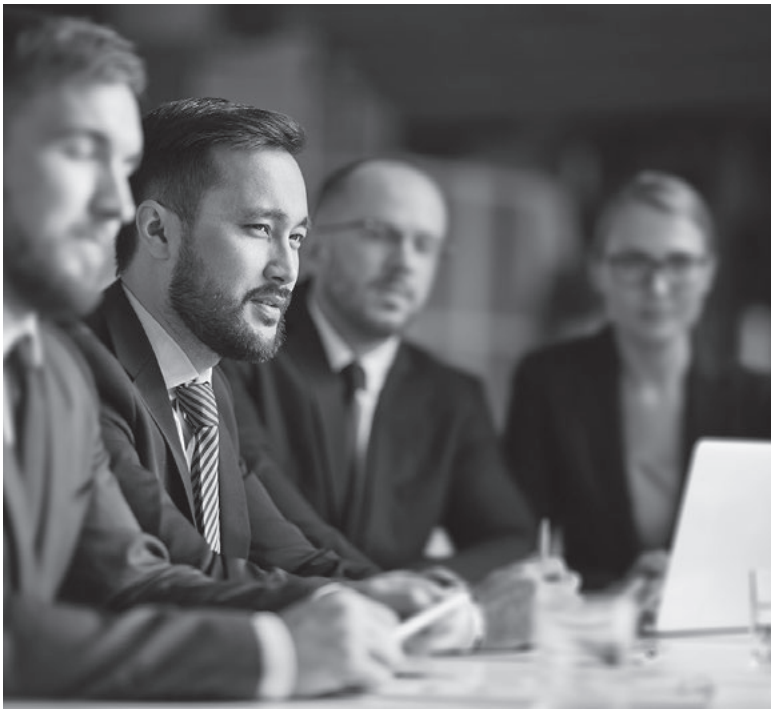
While it will ultimately carry out the fight, delegating cybersecurity entirely cuts senior management out of potentially catastrophic decisions. Executive prioritization and support for cybersecurity controls risk exposure in six key areas:

- Valuation and the Bottom Line
- Critical Enterprise Assets and Operations
- Reputation, Relationships, and Trust
- Safety, Compliance, and Liability
- Performance and Competitive Ability
- 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 as intellectual property, confidential data, reputation, and relationships.

Cyberattacks have destroyed more than $1 trillion of intellectual property and confidential information value. 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, cybersecurity is not just an IT problem. Cyberattacks 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.



Core Security Solution

Core Security 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. Core Security identifies the severity and intent of these attacks even when the malware evades detection.

Advanced Threat Detection

Get complete visibility into network threat-related activities in your organization. Core Security provides advanced threat detection products and the market-leading security information and event manager (SIEM) offering, giving you actionable intelligence and context needed to manage security

risks across your enterprise. Our solutions enable you to reduce the risk of compromise by uncovering vulnerabilities, wherever they reside within your environment, and work together to make sure you focus attention where it matters most. Reduce your threat surface and find out which devices are most susceptible to attacks within your organization.

Our solutions enable you to reduce the risk of compromise by uncovering vulnerabilities, wherever they reside within your environment.

coresecurity
by HelpSystems

www.coresecurity.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.