

Cyber Theft of Corporate Intellectual Property:

The Nature of the Threat

Economist Intelligence Unit

**The
Economist**

*An Economist Intelligence Unit
research program sponsored by
Booz Allen Hamilton*

Booz | Allen | Hamilton



List of Interviewees

ASHAR AZIZ Founder and CEO of FireEye

JOEL BRENNER Former US national counterintelligence executive and author of *America the Vulnerable*, currently an attorney at Cooley LLP

RONALD DEIBERT Director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs at the University of Toronto

JAMIL FARSHCHI Former chief information security officer at Los Alamos National Laboratory, now senior business leader of strategy, planning, and initiatives at Visa

JOHN MEAKIN Former director of digital security and CISO at BP plc, now global head of solutions at Deutsche Bank

ALAN PALLER Director of research at the SANS Institute

CHRIS PORTER Principal on Verizon's Research Investigations Solutions and Knowledge Team

EUGENE H. SPAFFORD Professor of computer science at Purdue University

JOHN STEWART Chief security officer at Cisco

PEIRAN WANG Visiting researcher at the Center for Economic Law and Governance, Vrije Universiteit Brussels

About the Survey

In March of 2012, the Economist Intelligence Unit conducted a global survey, sponsored by Booz Allen Hamilton, of 352 executives to assess attitudes toward the cyber theft of intellectual property. Forty-two percent of survey respondents are board members or C-level executives, including 95 CEOs. The respondents are based in Asia-Pacific (29 percent), North America (31 percent), Western Europe (28 percent), Middle East and Africa (6 percent), Latin America (3 percent), and Eastern Europe (3 percent). More than half of the survey respondents (52 percent) work for companies with global annual revenues exceeding US \$500 million. Twenty-one different industries are represented in the survey sample, including healthcare (13 percent), aerospace/defense (12 percent), professional services (12 percent), government/public sector (10 percent), IT and technology (10 percent), and financial services (10 percent).

Contents

Executive Summary.....	2
Introduction	3
Section 1: The Current Landscape.....	4
A Lack of Corporate Awareness.....	6
The Sources of the Attacks.....	8
The Government Response	9
Business Views on Sources of Attacks.....	11
Section 2: The Long-Term Implications	14
Section 3: The Corporate and Government Response.....	16
Conclusion	20
About Booz Allen	21
About Economist Intelligence Unit	21

Executive Summary

- **THE SECURITY OF ALL CORPORATE INTELLECTUAL PROPERTY (IP) IS NOW UNDER CONSTANT ASSAULT.** The attackers include competitors, organized criminal groups, disloyal insiders, “hacktivists,” and the agents and associates of governments.
- **EXPERTS SAY THE ATTACKS HAVE PENETRATED VIRTUALLY EVERY MAJOR CORPORATION.** Many victims still have no idea what IP thieves have taken. And although companies are ramping up defenses, more attacks are succeeding.
- **THE THREAT POSES SERIOUS LONG-TERM CONSEQUENCES TO COMPANY PROFITABILITY AND COMPETITIVENESS.** It could also upset the value of national industries and remap the economic, political, and military landscape.
- **OUR SURVEY OF CORPORATE EXECUTIVES INDICATES THAT A LARGE SECTION OF THE BUSINESS COMMUNITY MAY NOT YET FULLY APPRECIATE THE THREAT THESE ATTACKS POSE.** Respondents believe attacks are less widespread, less successful, and less threatening than experts indicate.
- **WESTERN GOVERNMENTS HAVE REVAMPED THEIR INTELLIGENCE STRATEGIES TO MEET THE THREAT AND HAVE BEGUN SHARING INFORMATION WITH EACH OTHER AND WITH CORPORATE OFFICIALS.** But international law enforcement has had limited success and discussions with China and Russia have ended in gridlock.
- **A SOLUTION REQUIRES GREATER COMMUNICATION BETWEEN THE PUBLIC AND PRIVATE SECTORS ABOUT THREATS AND BREACHES.** Industry must focus on securing its systems and be more forthcoming about break-ins, while governments must engage each other and the private sector to meet the technical, legal, and diplomatic challenges of creating a secure Internet. ••

Introduction: The Magnitude of the Challenge

MANY CORPORATIONS LIVE OR DIE ON THE STRENGTH OF THE INTELLECTUAL PROPERTY

THEY CREATE. A set of plans for a new airplane or a piece of proprietary software developed over several years is often worth many times more than all of the physical property on a company's balance sheet. As a result, the theft of a single piece of IP has the potential to destroy the competitive advantage a company has built up over decades.

Today, the security of all corporate IP is under constant assault. Corporate computer systems around the globe are being attacked by hackers seeking IP and other valuable business information.

THE INVADERS ARE MANY. There are the profiteers: unscrupulous competitors, organized criminal groups, and disloyal insiders. There's an emerging class of politically motivated "hacktivists." But perhaps most troubling are the agents and associates of governments like China and Russia, who are engaging in economic espionage aimed at fast-tracking their economic development and boosting their political and military power, according to security experts and Western intelligence agencies.

Some experts argue that years of attacks have already led to massive transfers of wealth-generating innovations to rivals, with grim consequences for advanced economies in the decades ahead. According to an oft-cited 2009 estimate by security software firm McAfee, a unit of Intel Corp., rampant IP theft is costing companies a trillion dollars a year. However, the true size and

shape of the crisis is unknown because the vast majority of security breaches go unreported by embarrassed and anxious victims and because measuring losses is exceedingly tough. Yet the problem is clearly worsening, as the opportunities for cyber theft multiply with each technological advance and as attackers gain in sophistication.

Two years of alarming headlines about break-ins at the likes of search giant Google, EMC Corp.'s RSA security unit, and defense contractor Lockheed Martin are having their effect. More corporate executives and government officials now realize that even the best-defended networks buckle under high-octane assault and have begun to address the problem. Although they have yet to agree on the best way forward, the protection of corporate IP has moved to the top of business and government agendas.

Section 1:

The Current Landscape

A GLOBAL PROBLEM

Companies that think they're unlikely to be attacked are deluding themselves. Security experts say that companies of all stripes around the world are being threatened by skillful cyber attacks designed to steal business secrets. "If you have anything of value, you will be targeted. You won't necessarily know by who," says John Stewart, the chief security officer of technology giant Cisco Systems.

The top targets are the engines of today's world economy and drivers of its geopolitical rivalries: the information-technology, oil and gas, defense, and pharmaceutical industries, and the law firms and consultancies that serve them. "In the last decade or so, we've seen a dramatic increase in economic espionage, both commercial and state-sponsored," says Joel Brenner, former US national counterintelligence executive and author of the book *America the Vulnerable*. "The US is the biggest, fattest target," he says, but, "this is not just a US problem."

THE TYPES OF THREATS

Companies now face a multiplicity of attacks on their networks, from the mundane to the highly sophisticated. The vast majority of malicious activity on corporate networks is the worker-bee hum of ordinary malware, common to both corporate and home computers, that's designed to gather financial details from PCs for fraud schemes. Much of this activity is orchestrated by organized crime groups in Eastern Europe.

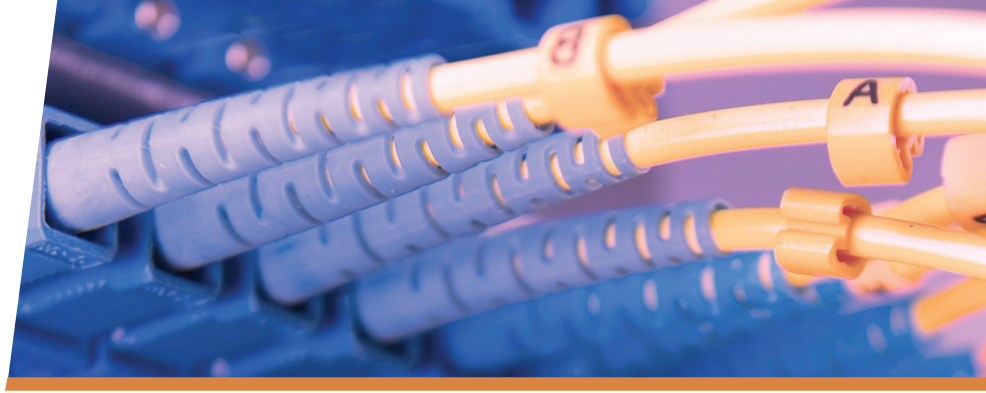
But much more perilous are targeted attacks, which use similar tools but are designed for more

insidious purposes, such as stealing IP. Typically, they begin with a relatively low-tech con, often a personalized e-mail known as a "spearphish" that leverages knowledge of the recipient or his company, often gleaned from social networks, to trick him into opening an attachment or visiting a website that deposits malware on his computer.

In the most sophisticated scenarios, the e-mails are highly researched and crafted to raise no suspicions. The malware silently installs itself by exploiting unknown software flaws, dubbed "zero-days" for the amount of time security professionals had to respond: none. Because the flaws and the malware used have never been seen before, traditional defenses like antivirus software that are designed to stop known attacks are useless.

With this foothold into the company, the hacker hopscoches quietly through the network, finds valuable data, and spirits it away. High-level hackers working inside high-value networks have been known to carefully plan their invasion and to stick around and pilfer data for months and even years in a type of attack that has been dubbed an "advanced persistent threat," or APT, and typically involves state-sponsored actors, according to Western intelligence agencies. Some dig so deeply, "you can't find them with any of the tools we have today," says Alan Paller, director of research at the non-profit SANS Institute, an association of technical security professionals.

Attacks like these have felled the great and the powerful. In 2009, some 30 companies including Google were hit by so-called Operation Aurora, which Google first disclosed in January 2010 and



said originated in China. Also in 2009, Chinese hackers are believed to have attacked at least five multinational energy and petrochemical companies and harvested sensitive information about their operations and contract bids, in an operation revealed by McAfee and dubbed Night Dragon.

Even a top network security company was compromised. In March 2011, US-based RSA said it suffered a break-in that resulted in the theft of IP related to its popular SecurID product, which many companies use to keep unauthorized users out of their own networks. In June, Lockheed Martin said the theft at RSA enabled a breach of its network. A little later that month, the International Monetary Fund, which possesses market-moving information on sensitive topics like bailouts of countries facing economic crises, said it was hit with a sophisticated cyber attack.

MORE ATTACKS ARE SUCCEEDING

Although targeted attacks amount to a small percentage of malicious activity on corporate

computer systems, large corporations now sustain anywhere from a dozen to hundreds of successful targeted attacks every week, according to Ashar Aziz, founder of FireEye Inc., a security firm that protects many large corporate and government networks from advanced attacks. Aziz's firm has detected advanced targeted attacks on companies across North America, Europe, Asia, and the Middle East, and he expects companies in China and Russia are compromised, too. "I'm sure there are nation-states on the other side infiltrating them—spy versus spy."

Companies may have ramped up defenses, but more attacks are succeeding. In the past, large corporations tangled with perhaps one or two major incidents a year, says John I. Meakin, the former chief information security officer of BP plc who is now global head of security solutions at Deutsche Bank. "Now one a month is probably the norm." One survey respondent stated his belief simply: "If you are stupid enough to put valuable IP online, it can (and probably will) be stolen."

"If you have anything of value, you will be targeted. You won't necessarily know by who," says John Stewart, the chief security officer of technology giant Cisco Systems.

A Lack of Corporate Awareness

MOST SECURITY CONSULTANTS interviewed for this article believe that the private sector has failed to pay sufficient attention to the threat IP theft poses. A recent EIU survey of global senior executives indicates that the corporate world may not be completely aware of the problem. While 69% of respondents say that IP-related cyber attacks either occur regularly or are rampant, 22% believe the attacks are rarely successful and 9% consider concerns about IP to be overblown. Only 13% of companies believed that most companies have had IP compromised in a serious way thanks to a cyber attack.

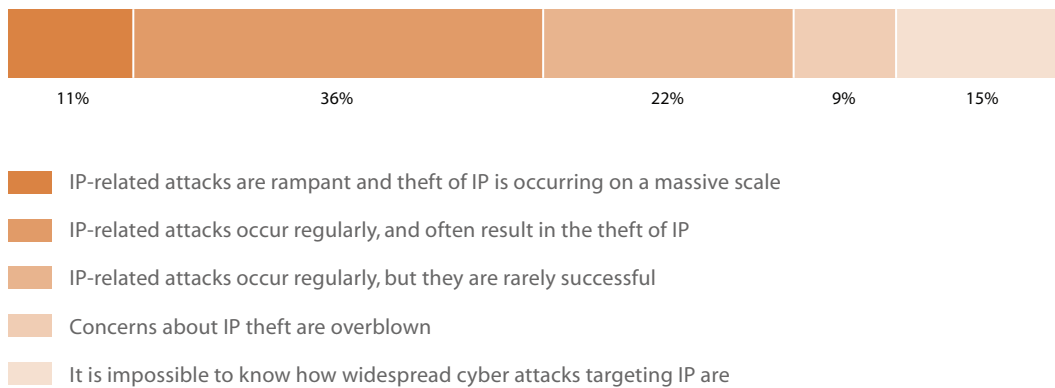
The survey results indicate that respondents may not be aware of breaches they have suffered or the extent of the damage. Only 22% of private sector respondents say that they've suffered some type of IP theft and only 3% of those attacked say that their company's competitiveness and profitability was harmed. 15% said that the incident was serious but that they were able to handle it and therefore

suffered little damage. 4% say that the consequences remain unknown.

Acknowledgement of serious attacks varied significantly by sector. 31% of respondents from the pharma/biotech sector acknowledged that they had suffered a serious breach, the highest of any industry sector. Respondents from the defense industry came in second (24%) followed by financial services (21%). Only 14% of respondents from IT and tech admitted experiencing a serious attack.

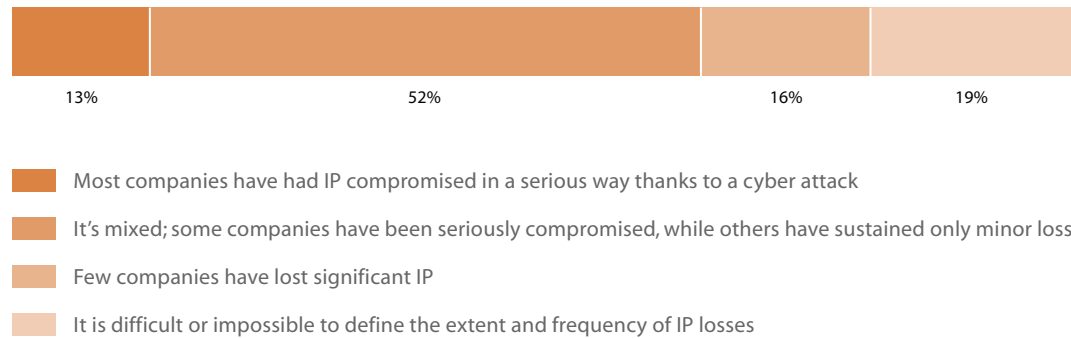
Public sector respondents to the survey appear to take the problem more seriously and share the concerns of security consultants: 53% believe that the private sector has not understood the scale of the problem of IP theft by cybercriminals. 69% of the public sector respondents also believe the private sector does not share sufficient information with government about vulnerabilities.

FIGURE 1 In your opinion, how frequent are cyber attacks focused on the theft of intellectual property (IP), such as trade secrets, product designs, or other proprietary information?



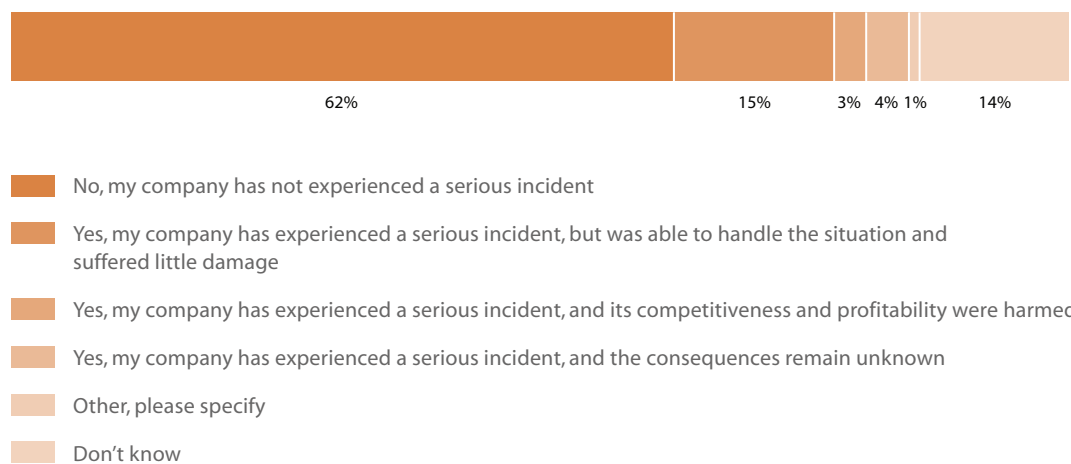
Source: Economist Intelligence Unit survey, March 2012

FIGURE 2 How widespread do you consider the theft of corporate IP via cyber attacks?



Source: Economist Intelligence Unit survey, March 2012

FIGURE 3 Has your organization suffered significant IP theft?



Source: Economist Intelligence Unit survey, March 2012

The Sources of the Attacks

TRYING TO DETERMINE THE SOURCES of these attacks against IP can be difficult because sophisticated hackers are often able to avoid detection and hide their tracks. Their targeted attacks stay under the radar by quietly penetrating the outer shells of networks, unseen by traditional security technologies. Then they can typically move inside unfettered by further controls. Moreover, most companies don't have tools for detecting malicious activity within their networks or sensitive data exiting their network. If companies do discover they've been infiltrated and lost IP, it's typically months or years later, and almost always because a law-enforcement agency comes knocking, experts say. "The unnoticed threat is the most dangerous," added one respondent from our survey.

Companies that do uncover attacks often never discover who attacked them. Many are absorbed with stopping and cleaning up the attack and don't attempt to find its source. Even when companies or government authorities mount a probe, investigators often cannot prove definitively who the attackers were, says Chris Porter, principal on Verizon's Research Investigations Solutions and Knowledge Team. Investigators can often trace them through the Internet for a time, he says. But hackers have multiple tools for preserving their online anonymity, and "at some point it [the trace] just disappears."


However, the governments of a number of countries with companies that have been victimized have pointed fingers at China and

Russia. The US intelligence community in an October 2011 report to Congress publicly accused those two nations of aggressively collecting information as part of a strategic competition with the US. The Chinese "are the world's most active and persistent perpetrators of economic espionage," the report by the Office of the National Counterintelligence Executive (NCIX) said, and Russia's intelligence services are a second major culprit. These governments use their own hackers as well as independent hackers to supplement their capabilities and provide "plausible deniability," it said.

The intrusion at Google, which led to theft of source code, may be illustrative. Investigators reportedly traced the attack to computers at two educational institutions in China—a university with a top computer science program and a vocational school with ties to the military and to Baidu, China's most popular search engine and a Google competitor.

The NCIX report added that some US allies with advanced cyber capabilities also engage in economic espionage, although mainly through old-fashioned human intelligence. Experts point to France and Israel, but say the extent of their activity is minimal compared to China and Russia. Some hacking on behalf of Iran has also been documented.

Experts also point their fingers at criminal groups. Typically, they work as hackers for hire by unscrupulous competitors, but some may



The Chinese “are the world’s most active and persistent perpetrators of economic espionage,” the report by the Office of the National Counterintelligence Executive (NCIX) said, and Russia’s intelligence services are a second major culprit.

hack first and sell what they find to the highest bidder (or use it themselves for extortion). “There’s an enormous amount of corporate espionage. It’s huge, but nobody’s got their arms around it,” says the SANS Institute’s Paller. Sometimes state-sponsored actors and cybercriminals cooperate. In underground marketplaces, cybersecurity firms say they have seen criminal hackers selling access to specific companies’ networks, and suspect that state-sponsored actors have been buyers.

Disgruntled employees, laid-off workers, and dishonest business partners also steal IP to damage companies or deliver secrets to a competitor in exchange for money or a new job. US prosecutors have won several convictions of corporate insiders linked to China who stole IP belonging to US employers and delivered it to Chinese competitors. In one prominent incident, Yu Xiang Dong, a product engineer at Ford Motor Co., was sentenced to 70 months in prison for copying 4,000 Ford documents onto an external hard drive and delivering them to Chinese car maker Beijing Automotive Co., where he subsequently obtained a job.

And finally, there is the rising threat of hacktivism. Intrusions tied to politically motivated activist groups such as Wikileaks, Anonymous, and LulzSec have emerged in the past year to target sensitive information, such as e-mails. A spate of attacks targeted defense contractors and firms like Sony that hacktivists saw as showing careless disregard for consumers’ personal information. Apparently inspired by protest movements that took flight around the globe, most of these attacks were designed to embarrass their targets publicly, not to benefit competitors or enrich the attackers themselves.

If companies do discover they’ve been infiltrated and lost IP, it’s typically months or years later, and almost always because a law-enforcement agency comes knocking, experts say.



Business Views on Sources of Attacks

BUSINESS LEADERS IN THE EIU'S SURVEY HAD SIGNIFICANT DIFFERENCES of opinion about the source of the attacks. Sixty percent of North American respondents described state-sponsored attacks as being frequent or very frequent. This is much higher than respondents from Asia-Pacific (42%) and Europe (41%). North American respondents also believed that hacktivists were more likely to be the source of attacks than respondents from Europe or Asia-Pacific.

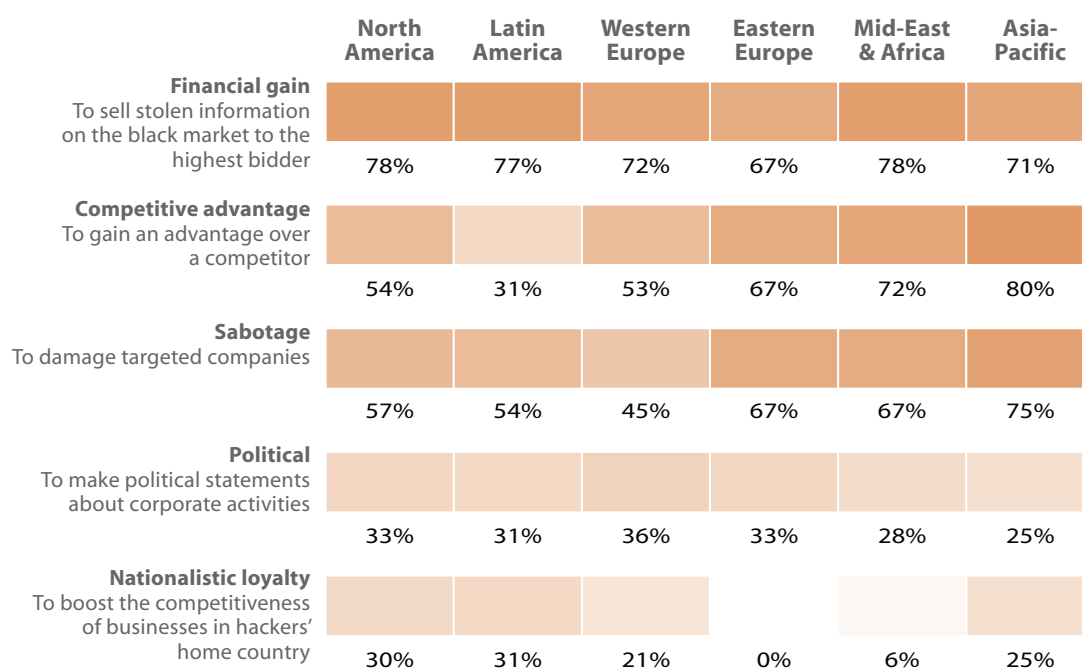
Respondents from Asia-Pacific, by contrast, were more likely to blame former employees than respondents from North America or Europe. Eighty percent of respondents of companies headquartered in Asia-Pacific believe that gaining a competitive advantage is more important than financial gain. However, only 53% and 54% of respondents headquartered in Europe and North America, respectively, cite this as a motivator. Respondents from Asia-Pacific also give more weight to sabotage as a key motivator, selected by 75% of respondents, versus 57% of North American respondents and 45% of European respondents.



Some respondents expressed some skepticism about attempts to blame particular countries for IP theft. Twenty-nine percent of respondents believed that attempts to blame particular countries for stealing corporate IP are politically motivated. Respondents who agreed with this position were more often found in Asia-Pacific (40%) than Europe (26%) or North America (24%).

Some survey respondents have also expressed doubts about the motivations of security consultants as well: "In real terms, we wonder if this threat is now more talked about than ever before," said one respondent. "Is this a new area for technology to make money?"

FIGURE 4 What are the main motivating factors behind the theft of corporate IP?



Source: Economist Intelligence Unit survey, March 2012

Section 2: The Long-Term Implications

THE THREAT TO BUSINESS

The theft of business secrets can pose a number of serious consequences to a company, regardless of who's responsible. Its reputation with customers, partners, and suppliers may be tarnished, and this eroded trust could hurt its market position and ability to win new business. A breach could lead to costly and damaging lawsuits. And companies in industries like finance, energy, and healthcare may tangle with regulators.

But perhaps most gravely, a company's long-term profitability and ability to compete in the marketplace could be seriously impaired if it loses information critical to its value proposition or operations. For example, stolen product blueprints could enable rivals to build clones and sell them at a lower price.

Some companies that have suffered IP theft have sustained considerable damage, though the extent isn't always clear. The theft of data related to RSA's flagship SecurID product led to a reported exodus by some customers and speculation about RSA's survivability. The string of break-ins at Sony last year contributed to a steep decline in its stock price, though factory halts following Japan's 2011 earthquake and tsunami and earnings strains due to the outsized strength of the yen also dragged on its shares.

But perhaps the most troubling case is Nortel Networks, the now bankrupt telecommunications gear maker that was once Canada's largest company. Its computer systems were reportedly compromised for over a decade by hackers likely from China. Speculation had swirled since 2004

that Chinese telecom giant Huawei Technologies was copying Nortel's hardware and instruction manuals. Now, people are speculating that IP theft may have been central to the company's downfall.

Companies that focus on short-term security and profitability can no longer afford to ignore the threat that IP theft poses to their long-term security and profitability.

THE LONG-TERM GLOBAL THREAT

If the looting of corporate networks continues apace, as security experts and concerned governments predict it will, the damage will inevitably stretch beyond the fortunes of individual companies. Taken to an extreme, it could upset the value of national industries and even fundamentally remap the economic, political, and military landscape.

The concentration of IP attacks inside the technology, energy, defense, and drug industries makes it clear that these sectors are the key economic battlegrounds of the future. And the battles have already begun. "Espionage is contributing significantly to the tidal flow of capital, intellectual and otherwise, from West to East," says Joel Brenner, a former US national counterintelligence executive who is now an attorney at Cooley LLP. "It's not the most important contributor, but it is significant."

Security experts say China's espionage program is driven by its hunger for economic growth and energy sources to meet the needs and aspirations of its growing population and exploding middle class, and for military technology to bolster its

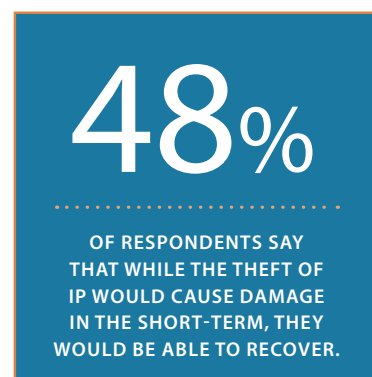
armed forces. According to the NCIX report, a particular policy goal is to close a gap with the West in science and technology, and in 1986 China launched a program called Project 863 with the explicit aim of “catching up fast and surpassing” Western powers in that realm.

But not everyone thinks China is a major cyber threat. Peiran Wang, a visiting researcher at Vrije Universiteit Brussels, says China still has major struggles with cyber defense and is skeptical it has the technical abilities to carry out significant offensive cyber operations. He also doubts espionage can meaningfully aid China’s mission to become a great power. Which isn’t to say China won’t challenge the West in cyberspace. Chinese nationalists have argued the country must fight US domination of cyberspace and the neocolonial export of its values and culture, he says, and that may impact government thinking.

Russia’s own espionage effort is also driven by a desire to diversify its economy and reduce its dependence on natural resources, according to the NCIX report. Russia too has a sense of grievance; it believes the global economic system is tilted in the favor of Western countries at its expense. Though Russia has denied hacking, it has enlisted its intelligence services to help carry out its economic policy goals. The director of Russia’s Foreign Intelligence Service, Mikhail Fradkov, said in December 2010 that it “aims at supporting the process of modernization of our country and creating the optimal conditions for the development of its science and technology.”

IP theft threatens some companies more than others. Companies that are less dependent on IP for competitive advantage may be able to recover fairly quickly. Indeed, the EIU’s survey shows that many executives are optimistic about their companies’ abilities to respond to IP attacks, with 48% of respondents saying that while the theft of IP would cause damage in the short-term, they would be able to recover. Companies that innovate quickly—and develop new IP—may find that they continue to outpace also-ran competitors who have tried to steal their older ideas.

In the most alarmist scenarios, however, IP theft by low-cost competitors manifests itself only years later in reduced industry competitiveness, slower economic growth, lost jobs, and even lower living standards. By the same token, defense technologies and secrets stolen from US industry and government networks could give China and Russia military advantages worth billions.



Section 3: The Corporate and Government Response

CORPORATE VERSUS GOVERNMENT RESPONSIBILITY

Much of the responsibility for defense against cyber theft of IP lies at the feet of companies, owners of the networks under assault. Many are stepping up their efforts to secure their computer systems, which are proving all too easy to compromise.

But it's equally clear that no corporation is capable of defending its network against the full universe of cyber threats. When a company is targeted by high-level hackers backed by a country, "it's not a fair fight," says Cisco's Stewart. Many experts say national and international authorities must step up efforts to combat cybercrime using all available legal, diplomatic, and enforcement tools.

INTERNATIONAL EFFORTS AGAINST IP THEFT

A number of Western governments have revamped their intelligence strategies to meet the threat of cyber espionage. For instance, Australia, France, and the UK have established new units to coordinate policy and intelligence activities. And many of these governments, recognizing that much of their

national infrastructures are privately owned, have begun sharing more information about threats through industry groups and directly to corporate executives, says Deutsche Bank's Meakin. US, French, and German authorities all reportedly offer regular threat briefings to companies.

International cooperation against IP theft has also improved. Many international organizations from the United Nations to the International Telecommunication Union to the Council of Europe are tackling elements of cybersecurity policymaking, with varying degrees of success. Experts argue the most capable should be bolstered as top forums for dialogue and for creating multilateral strategies with input from national governments, non-governmental groups, and the private sector.

International law-enforcement organizations have produced important prosecutions of cybercriminals and insiders. By involving law enforcement, companies stand a better chance of finding out who attacked them and how, which is vital to understanding the threats and mounting better defenses.

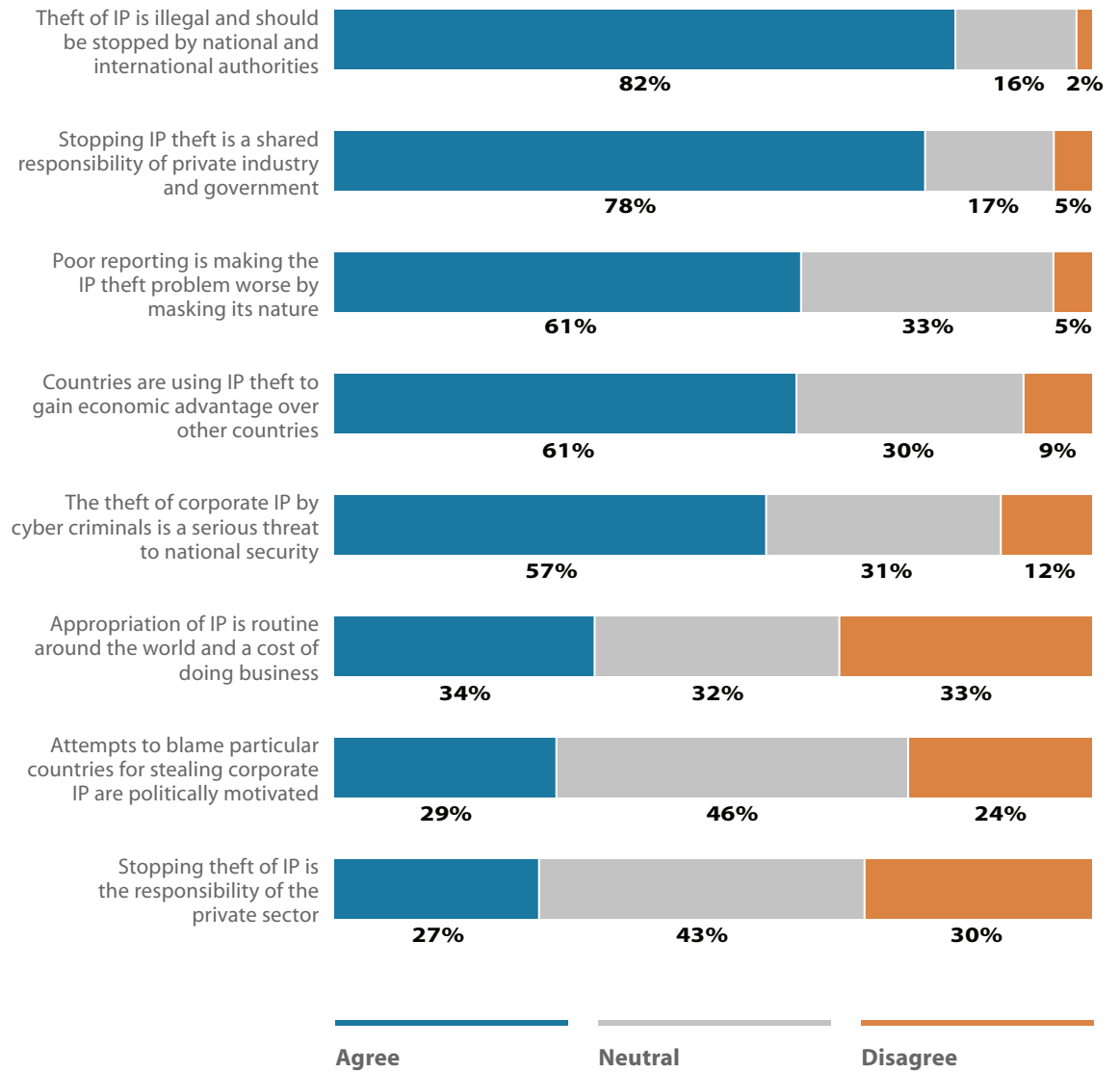
But international law enforcement has its limits. German prosecutors launched 31 preliminary proceedings on espionage cases in 2007 but won only one arrest and conviction, with cases often foundering on diplomatic immunity and difficulties of decisively proving culpability. Cross-border cooperation between law enforcement agencies in hot spots like China and Russia is also extremely limited. Many agencies lack the skills and resources to investigate the flood of incidents. And when they do investigate, arrests and prosecutions can take years, if they happen at all, hampering any deterrent effect on emboldened hackers.

Western governments and their allies are cooperating more closely than ever on cybersecurity. They meet regularly at conferences to discuss the issues, and US officials have reportedly ramped up their links with military and civilian agencies across NATO and the Western world. But efforts at detente with China and Russia have faltered. Those nations hold a different and more authoritarian view of Internet security that calls for more control over online speech, which clashes with Western values. They have hotly

denied involvement in cyber theft of commercial property and claimed that they, too, are victims of hacking. And with an array of Chinese governmental bodies involved, “you cannot count on a coherent strategy or policy towards cybersecurity from China,” says Peiran Wang.

The EIU’s survey demonstrates broad agreement on the steps that should be taken. Seventy-eight percent of respondents said responsibility for stopping IP theft should be a shared responsibility of private industry and government. There was also broad agreement that governments should provide Internet service providers with information to help them combat attacks (72%), that regulators should play a role in requiring companies to disclose information about attacks (69%), and that securities regulators should require companies to disclose attacks that have an impact on shareholder value (64%).

FIGURE 5 Do you agree or disagree with the following statements?



Source: Economist Intelligence Unit survey, March 2012

***THE THEFT OF
A SINGLE PIECE OF
INTELLECTUAL PROPERTY***

*HAS THE POTENTIAL TO DESTROY THE
COMPETITIVE ADVANTAGE A COMPANY
HAS BUILT UP OVER DECADES.*

Conclusion

THERE WILL BE NO EASY FIXES TO THIS COMPLEX AND GROWING PROBLEM.

But the threat to IP-dependent industries, the strategic sectors of developed economies, and even international political stability means addressing it is vital.

Standing up to the problem of cyber espionage requires the commitment of both industry and government, who must—and increasingly are—forging new approaches to defense and working together to meet emerging threats. While industry focuses on securing its systems, governments must further engage each other to meet the considerable technical, legal, and diplomatic challenges to creating a secure Internet.

The first step is improved communication; the public and private sectors must share more information with each other about cyber threats and security breaches. A better view would give both parties an improved chance of identifying and implementing effective technical responses and pursuing public policies—national and international—that can make a difference.

Ominously, survey respondents are divided about whether companies will be able to meet the security challenge in the future. More than half believe companies that fail to invest adequately in security will be hurt, and possibly fatally so. While half say effective defenses will emerge that are able to keep most organizations safe, 40% think most organizations will be unable to defend themselves. A majority—56%—say they don't have resources to meet the problem and another 17% say they have enough resources but they are not being used efficiently.

Is this a cry for help? We believe so.

About Booz Allen Hamilton

BOOZ ALLEN HAMILTON IS A LEADING PROVIDER of management and technology consulting services to the US government in defense, intelligence, and civil markets, and to major corporations, institutions, and not-for-profit organizations. Booz Allen is headquartered in McLean, Virginia; employs more than 25,000 people; and had revenue of \$5.59 billion for the 12 months ended March 31, 2011.

Booz Allen understands that cybersecurity is no longer just about protecting assets. It's about enabling organizations to take full advantage of the vast opportunities that the ecosystem of cyberspace now offers for business, government, and virtually every aspect of our society.

Those opportunities can be imperiled, however, by rapidly emerging cyber threats from hackers (hacktivists), organized crime, nation states, and terrorists. We help our clients in both business and government understand the full spectrum of threats and system vulnerabilities, and address them effectively and efficiently.

Booz Allen believes the key to cybersecurity today is integration – creating a framework that “thinks bigger” than technology to encompass policy, operations, people, and management as well. Through such a Mission Integration Framework, organizations can align these essential areas to address the real issues, and develop cyber strategies and solutions that keep pace with a fast-changing world.

To learn more, visit www.boozallen.com. (NYSE: BAH)

About the Economist Intelligence Unit

THE ECONOMIST INTELLIGENCE UNIT IS PART OF THE ECONOMIST GROUP, the leading source of analysis on international business and world affairs. Founded in 1946 as an in-house research unit for *The Economist* newspaper, we deliver business intelligence, forecasting, and advice to over 1.5 million decision-makers from the world's leading companies, financial institutions, governments, and universities. Our analysts are known for the rigor, accuracy, and consistency of their analysis and forecasts, and their commitment to objectivity, clarity, and timeliness.



Booz | Allen | Hamilton

Economist Intelligence Unit

The
Economist

*An Economist Intelligence Unit
research program sponsored by
Booz Allen Hamilton*