

Report based on
discussions with the

Security for Business Innovation Council

An industry
initiative
sponsored by
RSA



ABN AMRO

DR. MARTIJN DEKKER,
Senior Vice President, Chief
Information Security Officer

ADP INC.

ROLAND CLOUTIER, Vice
President, Chief Security Officer

AIRTEL

FELIX MOHAN, Chief Security
Officer

THE COCA-COLA COMPANY

RENEE GUTTMANN, Chief
Information Security Officer

CSO CONFIDENTIAL

PROFESSOR PAUL DOREY,
Founder and Director; Former
Chief Information Security
Officer, BP

EBAY

DAVE CULLINANE, Chief
Information Security Officer and
Vice President, Global Fraud,
Risk & Security

EMC

DAVE MARTIN, Chief Security
Officer

FEDEX

DENISE WOOD, Chief
Information Security Officer and
Corporate Vice President

GENZYME

DAVID KENT, Vice President,
Global Risk and Business
Resources

HDFC BANK

VISHAL SALVI, Chief
Information Security Officer and
Senior Vice President

JOHNSON & JOHNSON

MARENE N. ALLISON,
Worldwide Vice President of
Information Security

JPMORGAN CHASE

ANISH BHIMANI, Chief
Information Risk Officer

NOKIA

PETRI KUIVALA, Chief
Information Security Officer

NORTHROP GRUMMAN

TIMOTHY MCKNIGHT, Vice
President and Chief Information
Security Officer

SAP AG

RALPH SALOMON, Vice
President, IT Security & Risk
Office, Global IT

T-MOBILE USA

WILLIAM BONI, Vice President
and Chief Information Security
Officer, Corporate Information
Security

WITH GUEST CONTRIBUTOR:

MISCHEL KWON, Former
Director, U.S. Computer
Emergency Readiness Team
(CERT); President, Mischel Kwon
& Associates

WHEN ADVANCED PERSISTENT THREATS GO MAINSTREAM

*Building Information-Security Strategies
to Combat Escalating Threats*

RECOMMENDATIONS FROM GLOBAL 1000 EXECUTIVES



INSIDE THIS REPORT:

Key characteristics of
APTs

How enterprises are
making themselves
vulnerable

New approaches to
information security

Seven defensive
measures against
escalating threats



Report Highlights

APTs have moved from the realm of the military to the mainstream.

IN THE PAST 18 MONTHS, a string of highly sophisticated and targeted cyber attacks across the globe has revealed a seismic shift in the threat landscape.

TRADITIONALLY ONLY affecting the defense establishment, advanced persistent threats or “APTs” are now targeting enterprises in a wide range of industries.

OTHER THREAT ACTORS besides nation-states, including organized crime and “hacktivists,” have now achieved the requisite skills to carry out APT-style attacks.

ATTACKERS ARE MOVING beyond custodial data like credit cards to pursuing high-value digital assets such as intellectual property, access to mission-critical operations, and other proprietary data and systems.

TYPICALLY APTs ARE HIGHLY targeted, thoroughly researched, amply funded, and tailored to a particular organization—employing multiple vectors and using “low and slow” techniques to evade detection.

RATHER THAN GAIN ENTRY through the network perimeter, APTs prefer to gain entry by exploiting end users and end points. Social engineering and spear phishing are core tactics.

SEVERAL FACTORS ARE driving the rise of APTs including the fiercely competitive global economy and the declining market value of credit card numbers.

INHERENT WEAKNESSES IN IT and ineffective approaches to information security are making enterprises susceptible to APT-style attacks.

FOR MANY ORGANIZATIONS, tackling APTs will take fresh approaches and whole new ways of thinking about information security to combat this new class of threat.

CONFRONTING APTs WILL require giving up the idea that it is possible to protect everything. Security teams will have to focus on protecting the organization’s most critical information and systems.

THE DEFINITION OF successful defense has to change from “keeping attackers out” to “sometimes attackers are going to get in; detect them as early as possible and minimize the damage.”

THIS REPORT PROVIDES a valuable set of recommendations from 16 of the world’s leading security officers and an expert in APTs to help organizations build security strategies for today’s escalating threat landscape.

CONSIDER THAT NO organization is impenetrable. Assume that your organization might already be compromised and go from there.

SEVEN RECOMMENDATIONS in the report provide key ways to shore up defenses for organizations facing APTs. It will take not only the commitment of the information-security team but also the support of executive leadership.

ORGANIZATIONS ARE challenged to ask themselves tough questions about their security stance such as:

- Do we have the kind of intelligence-gathering and analysis capabilities that we need to keep up with the threats?
- Is our security monitoring actually looking for the right things?
- Would attackers be able to hijack administrative accounts?
- How many of our users would fall prey to a spear-phishing attack?
- Does executive leadership truly understand the nature of fighting a digital arms race?
- Are we using approaches to IT and security that make it easy for attackers?
- Do we have what it takes to fully leverage threat information from other organizations?

1

Introduction

S

ince the dawn of digital information, threats to that information have been increasing and security professionals have been adapting their strategies to keep pace. But in the past 18 months, we have been experiencing more than the typical incremental evolution in threats. We have been witnessing a seismic shift in the threat landscape.

A string of sophisticated cyber attacks—affecting pillars of industry and government—

has demonstrated an alarming level of proficiency in today’s cyber foes. Although “advanced persistent threat” or “APT” used to be a specialized term within the realm of military and defense experts, these incidents have pushed “APT” into the mainstream. Originally used to describe cyber espionage in which nation-states stealthily park themselves on a foreign government/contractor network over long periods of time in order to exfiltrate national



security secrets and defense data, the term APT has now broadened.

APT has come to mean a cyber attack that is highly targeted, thoroughly researched, amply funded, and tailored to a particular organization—employing multiple vectors and using “low

and slow” techniques to evade detection. While more conventional attacks might seek, for example, credit card data by “combing the neighborhood” for organizations that leave the proverbial back door unlocked, today’s advanced persistent threats focus



It is a very intelligent, well-armed, and effective foe that is fantastic at what they do, and it's going to take a new approach in most enterprises to combat it."

ROLAND CLOUTIER, Vice President,
Chief Security Officer,
Automatic Data Processing, Inc.



This changing threat landscape has generated a great deal of discussion in the information-security domain, including a fair amount of skepticism. Being cautious about a possibly over-hyped trend is reasonable; being dismissive about the current reality could be perilous. Smart organizations will recognize that the escalating threats warrant an evaluation of the risks and up-leveling of information-security strategies.

This eighth report from the Security for Business Innovation Council (SBIC) takes an in-depth look at what has changed in the threat landscape, discusses why enterprises are vulnerable, and offers a set of actionable

recommendations for managing the risks. It is based on the perspectives of 16 information-security leaders from Global 1000 organizations as well as a guest contributor who is a subject-matter expert on APTs.

Beginning in 2008, the SBIC report series has focused on the role of information security in enabling business innovation. The new breed of attacks aims directly at the heart of business innovation by pursuing core content such as intellectual property, trade secrets, business and manufacturing plans, R&D, market information, and access to mission-critical operations. At this juncture, building the right security strategies is essential for protecting an organization's future success.

on a specific purpose to obtain high-value digital assets or tap into critical systems.

The defense establishment has been experiencing these types of attacks for many years, but for other industries this is a new class of threat. The attackers have

set their sights on an expanding list of targets. It now seems that any organization with high-value digital assets is on the hit list. And, other threat actors besides nation-states are now capable of carrying out these types of attacks.

2

The Shifting Threat Landscape



The recent escalation of cyber attacks is creating headlines in IT publications, business journals, and even mainstream media. It's generating concern not only within information-security circles, but also executive ranks. Something about these attacks makes them even more startling than previous spates of data breaches—and it's not just the high frequency of incidents that makes them different.

Generally threats to information assets can be analyzed based on:

- Who: Who is conducting and/or directing the attacks?
- What: What specific organizations and information assets are they targeting?
- Why: What are their motives?
- How: What techniques do they use?

The current wave of cyber attacks indicates that in today's threat environment, all of these parameters

are dramatically shifting. (See chart "Conventional vs. Advanced Persistent Threats" on page 7.)

For example, organizations face an expanded array of attackers. Previously, most enterprises and government agencies faced a fairly wide spectrum of threats from so-called script kiddies to more organized cyber criminals. However, only those in national security and defense had to contend with threats at the very top of the spectrum. Now, more organizations in a wider range of industries are facing nation-state capabilities and other highly skilled threats.

It is difficult to draw a definitive line between "conventional threats" and "advanced persistent threats" since the distinction is not clear cut; it's more of a continuum than two absolutely distinct categories. It's also changing over time as adversaries expand goals and/or adapt techniques.



→ **APT-style attacks are typically:**

1. **HIGHLY TARGETED** – Tailored to a specific organization

2. **WELL-FUNDED** – Resource-intensive

3. **WELL-RESEARCHED** – With a focus on information about personnel

4. **DESIGNED TO EVADE DETECTION** – Refined "low and slow" techniques

5. **MULTI-MODAL AND MULTI-STEP** – Using multiple vectors, specifically gaining entry via end users and end points



Key Features

Advanced persistent threats typically share these distinguishing characteristics:

1. Highly targeted

The threat actors are focused on a particular goal. They carefully select their targets in order to pursue high-value digital assets. Their objective is more strategic in nature. Rather than seek credit card numbers and other custodial data, they pursue intellectual property, access to mission-critical operations, and other proprietary data and systems. (See chart on page 7 for more details.) Accordingly, their motives are no longer just quick pay outs but longer-term gains such as competitive advantage or sabotage. The attacks are designed specifically to defeat the target organization's existing security controls.

2. Well-funded

As determined adversaries, these attackers will spend the time and money required to get what they're after. If their attack methods are blocked by the organization's counter-measures, they quickly regroup and find a new way to circumvent defenses. They have access to highly developed, clandestine supply chains and the ability to procure malware, zero-day vulnerabilities, and computing resources.

Having the financial backing to wage resource-intensive, long-term attacks is most often attributed to nation-states. The actual perpetrators could be either directly under the command of nation-states or operating as service providers. Some organized-crime groups with the financial means now also have the motivation to carry out these types of advanced attacks, working for nation-state customers.

3. Well-researched

One of the hallmarks of APTs is reconnaissance. The threat actors conduct surveillance on the organization's personnel, IT infrastructure, and business processes. Armed with these details, they plan the attack. The focus of their investigation is typically learning the organizational structure and collecting personal details of employees and

partners. Social engineering and spear phishing are core tactics. Information is used to impersonate employees or trusted peers, getting people to reveal passwords, open infected email attachments, or click on malicious links. In addition, the attackers track down users with administrative-access rights in order to compromise their accounts and use the credentials to operate as privileged users.

The availability of personal and professional information on social-networking sites makes it easy for the attackers to obtain useful details on the organization and its people. They view an organization's employees as its weakest line of defense and easiest point of entry: often much easier than trying to defeat the network.

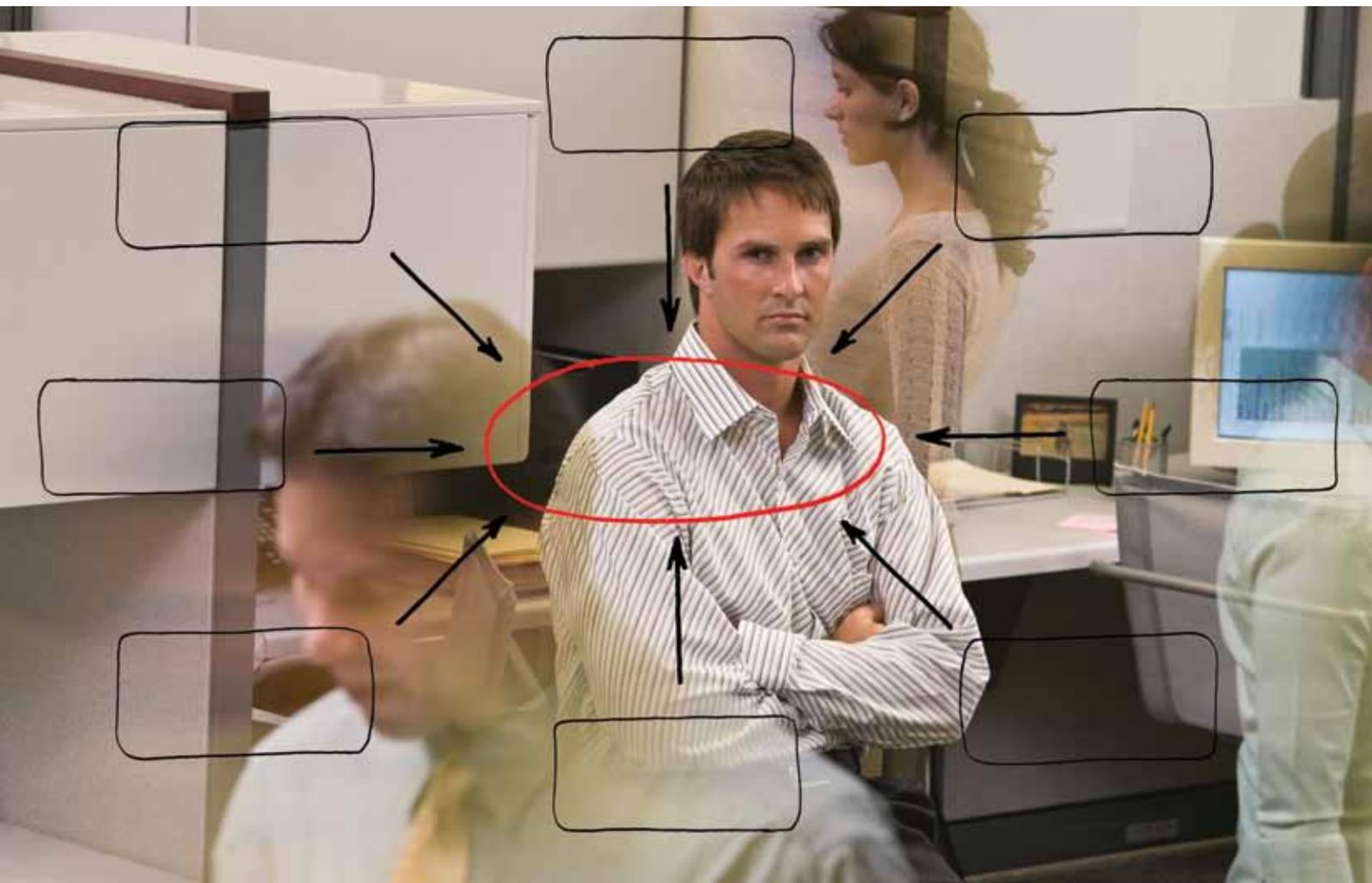
4. Designed to evade detection

Advanced persistent threats deliberately try to impede threat-detection mechanisms. For example, they use unique, novel attack patterns that are hard to identify with signature-based detection, short random broadcasts of information back to command and control that can avoid triggering an alarm, and encryption that obfuscates network traffic. It is common for attackers to distribute malware throughout an infiltrated IT environment and have it lie dormant for long periods of time until conditions are ripe for attack. Threat actors often aim for ongoing access to the network in order to come and go as they please and exfiltrate data whenever they want.



"ADVANCED PERSISTENT threats in the banking industry combine knowledge of malware with, for example, clever social engineering and a deep understanding of banking. Advanced persistent threats have a high degree of organization bringing together different people with different skills."

DR. MARTIJN DEKKER, Senior Vice President,
Chief Information Security Officer, ABN Amro



5. Multi-modal and multi-step

Their typical method of attack uses multiple vectors including social engineering, application-layer exploits, zero-day malware, and highly developed data-exfiltration techniques. The attacks are meticulously planned and occur in stages over time. Obviously no two attacks are the same and methods vary widely, but it is possible to illustrate a set of common steps:

1. Reconnaissance to build knowledge of the organization
2. Social engineering and/or spear phishing to target end users
3. Exploitation of vulnerabilities in an end point
4. Lateral expansion using peer relationships to roam the network
5. Escalation of privileges –
Additional spear phishing or decrypting administrators' passwords
6. Compromise of internal systems
7. Exfiltration of data or other objective (such as planting false information)
8. Cleanup



←		CONVENTIONAL THREATS vs. ADVANCED PERSISTENT THREATS	→
		+	ADDITIVE:
Who are the attackers?	Opportunistic hackers or cyber criminals		Well-resourced and determined adversaries: nation-states (and associated groups), globally connected organized crime, nefarious corporations, hacktivists
What data do they target?	Custodial data: credit card data, bank account data, personal information Generically valuable information that could be used by or sold to many interested parties		High-value digital assets: intellectual property, national-security data, trade secrets, source code, R&D material, market and customer information, financial systems, business and manufacturing plans, access to mission-critical operations, and so forth Specifically valuable information that is pursued by or could be sold to a defined party
What organizations do they target?	Broad-based attacks on banks, card-data processors, online retail and services, general industry, and their customer bases		A selected organization in government, defense, oil & gas, energy, technology, financial services, and so on
Why?	Financial gain, identity theft, fraud, spam, recognition		Market manipulation, strategic advantage in national defense, economic advantage in an industry, competitive position in business negotiations, damage to critical infrastructure, politically driven causes
How?	Gain entry by attacking perimeter		Gain entry by exploiting end users and end points; carry out attack using multiple vectors
Malware used	Typically off-the-shelf malware Propagate malware as broadly as possible to improve the chances of landing in a profitable place		Often custom-designed or tailored malware Targeted use of malware in attacking one organization: to hijack systems, create diversions, establish back doors, and communicate with command-and-control servers
Skills	Technical skills		Reconnaissance: in-depth knowledge of an organization's people, business processes, and network topology
Reaction to countermeasures	Move to an easier target		Modify attack to pursue the target further

Signs of a Growing Menace

When an organization detects that they have been targeted by an advanced persistent threat, it is rarely publicly reported. Corporations and government agencies are not inclined to admit they've been compromised. Despite this reluctance, dozens of sophisticated, targeted cyber attacks involving major corporations have been reported in the news in the past 18 months. These are likely just the tip of the iceberg. Organizations in many industries have been affected including:

- Broadcast industry
- Critical infrastructure
- Defense industry
- Financial-services industry
- Governments worldwide
- Oil-and-gas industry
- Online-gaming industry
- Marketing-services industry
- Security industry
- Technology industry



In addition, government and national-security agencies around the globe have been tracking an increase in sophisticated threats and communicating their findings to industry.¹ National agencies in many countries have briefed boards of directors and executive leadership at large corporations in order to increase awareness and collaborate on plans to bolster public- and private-sector defenses.²

Recent research studies also show an escalation of threats. A study conducted by the Ponemon Institute found that “83 percent of respondents believe their organization has been the target of an advanced threat. 71 percent believe they have seen an increase in advanced threats over the past 12 months and 70 percent say that advanced threats suggest a new, more dangerous threat landscape.”³

There are several factors driving the escalation. Fundamentally, the global economy has become fiercely competitive and some players are resorting to illegal methods to gain the upper hand. Globalization has led to the interconnection of more and more systems; yet there are differing values and mores regarding the protection of intellectual property across the world. Having competitive threats is nothing new to corporations; what’s new is that

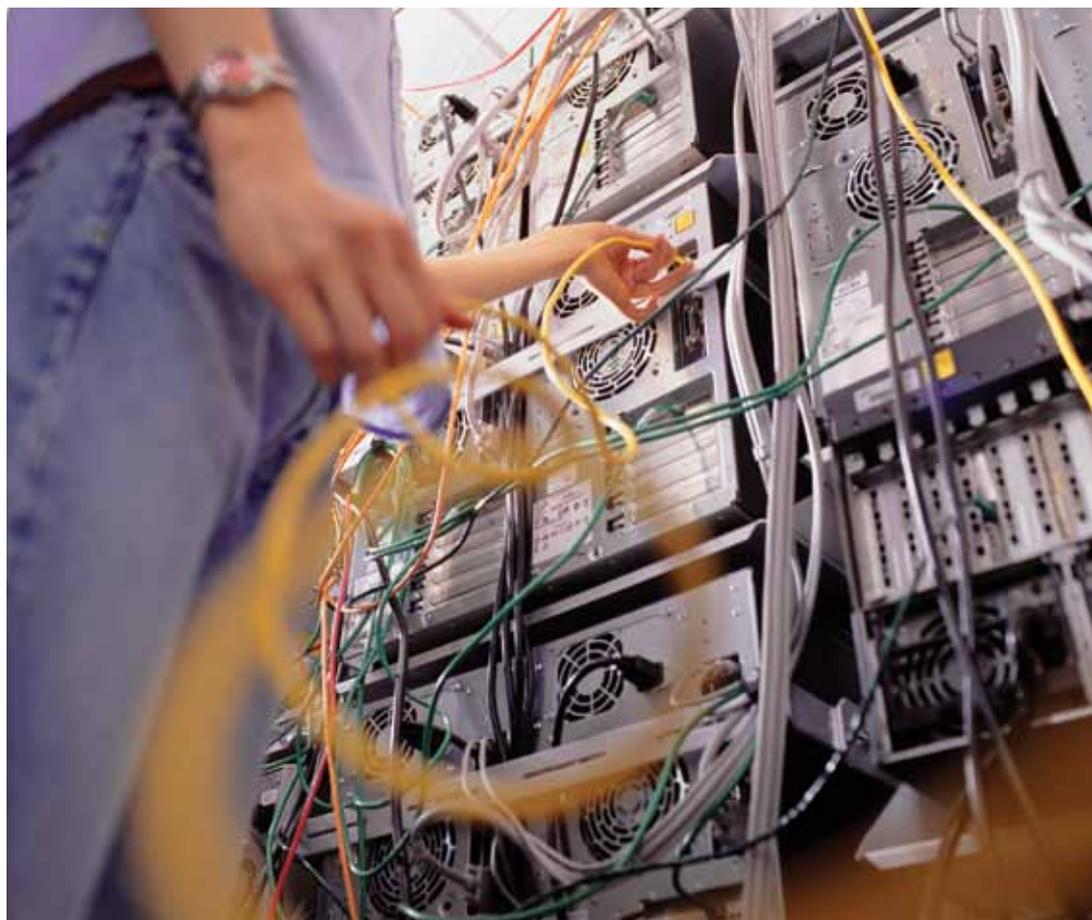
certain adversaries are now moving their espionage activities online. Currently, the barriers to accessing competitive information via network-based techniques are low—and the return on investment (ROI) is high. APT operators are exploiting this situation broadly across multiple sectors of the economy.

As well, the market for custodial data has become saturated. As the market value of credit card data declines, ambitious cyber criminals set their sights on other valuable information assets such as intellectual property and trade secrets that have the potential to become lucrative commodities.

Another factor is the proliferation of knowledge and skills among attackers. Just as in every field, know-how gets disseminated over time. Advanced persistent threats often get attributed to particular nation-states, but, in reality, the source of attacks can be difficult to locate as they are often rerouted through other countries. And at this point, it’s no longer just a few countries that have these capabilities, but many. Beyond nation-states, other threat actors such as organized crime and even politically motivated “hacktivists” are using similar techniques.

“The German Federal Office for Protection of the Constitution and the Federal Criminal Police Office have confirmed in their reports that there is increased activity regarding targeted, sophisticated attacks. These are coming from foreign countries’ agencies but also some criminal organizations are trying to get hold of IP from different companies.”

RALPH SALOMON,
Vice President, IT Security & Risk
Office, Global IT, SAP AG



¹ *Germany to set up cyber defense center in response to growing threats*, Infosecurity.com, December 28, 2010

² *Australia warns resource companies over cyber attacks*, cbronline, May 31, 2011

³ *Growing Risk of Advanced Threats*, Ponemon Institute, June 30, 2010

3

The Susceptible Enterprise

“THE FACT is there is very sophisticated, stealthy stuff running out there. So unless you’re looking for the right things, like connections out to the Internet, you’re not going to see this stuff.”

DAVE CULLINANE, Chief Information Security Officer and Vice President, Global Fraud, Risk & Security, eBay



Unfortunately, as the adversaries hone their skills, government agencies and corporations grow more susceptible.

Today’s IT environments at large enterprises have been built over many years, possibly decades. As organizations expand, merge, and develop global supply chains, they combine new and legacy systems, link networks, and integrate with more and more third-party service providers.

Inherent Weaknesses in IT

The current level of complexity in the enterprise IT environment makes it easy for skilled adversaries to hide and find either unknown or unpatched vulnerabilities. Adding to the complexity, employee-owned devices and social-media applications are entering the enterprise, creating new attack vectors.

Besides complexity, another weakness in enterprise IT is network design. Many enterprise networks are too flat. With a flat network design, all stations on the network can reach the others without going through any intermediaries such as bridges or internal firewalls. Having one broadcast domain costs less to manage and is more flexible than highly segregated networks. However, a flat network design facilitates attackers’ ability to roam the network and possibly reach high-value systems.

The number of application vulnerabilities also predisposes enterprises to cyber attacks. Many of today’s standard business applications have been developed over many years and contain millions of lines of code, making security holes inevitable. As well, often in-house or off-the-shelf applications are not built securely from the outset or are outliving the security of their components. The end result is that threat actors are able to find more and more vulnerabilities.

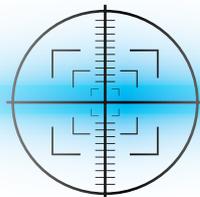
Ineffective Approaches to Information Security

Adding to the problem is that many security teams are not able to detect sophisticated attack patterns. Their conventional antivirus, firewall, and intrusion detection system (IDS) tools do not form a complete picture of an attack. The tools might identify an unauthorized access, a virus, phishing email, or piece of malware but do not associate these events. Also, signature-based detection methods don’t work well against APTs as the exploits are not well-known. Since log analysis was often implemented in response to regulatory demands, it has typically been tuned for compliance rather than threat mitigation.

Another limitation is organizational structure. Often the various groups responsible for security are too siloed and there is limited coordination among them. For example, those who are watching for events—the Computer Incident Response Team (CIRT) or Security Operations Center (SOC)—may not have complete information on the organization’s most important digital assets. Moreover, advanced persistent threats attack from multiple directions. They are not only IT-based but combine technical tactics with social engineering and/or physical access to a facility. Security teams cannot rely on silos of activity to accurately interpret multi-modal attacks.

“If the threat actors who have gone looking for zero-day vulnerabilities decide to monetize all the zero-day vulnerabilities they’re stockpiling, that might be an issue.”

DENISE WOOD,
Chief Information Security Officer and
Corporate Vice President,
FedEx Corporation



4

Recommendations



As advanced persistent threats pursue more targets, many organizations are starting to realize what they are up against. Industries that have dealt with these types of threats for years are further down the road in implementing specific defenses. However, most security teams have just begun to evaluate their position vis-à-vis the shifting threat landscape. It will take fresh approaches and whole new ways of thinking about information security to combat this new class of threat. (See chart on page 11, “Conventional vs. Advanced Approaches to Information Security.”)

For example, tackling advanced persistent threats means giving up the idea that it is possible to protect everything. This is no longer realistic. Security teams will have to work closely with the business to identify the organization’s most critical information

“FIRST OF ALL, classify your assets extremely well so that you understand what must be protected from a confidentiality point of view. Then you plan protection for those systems much more carefully than you would for some other systems.”

PETRI KUIVALA, Chief Information Security Officer, Nokia

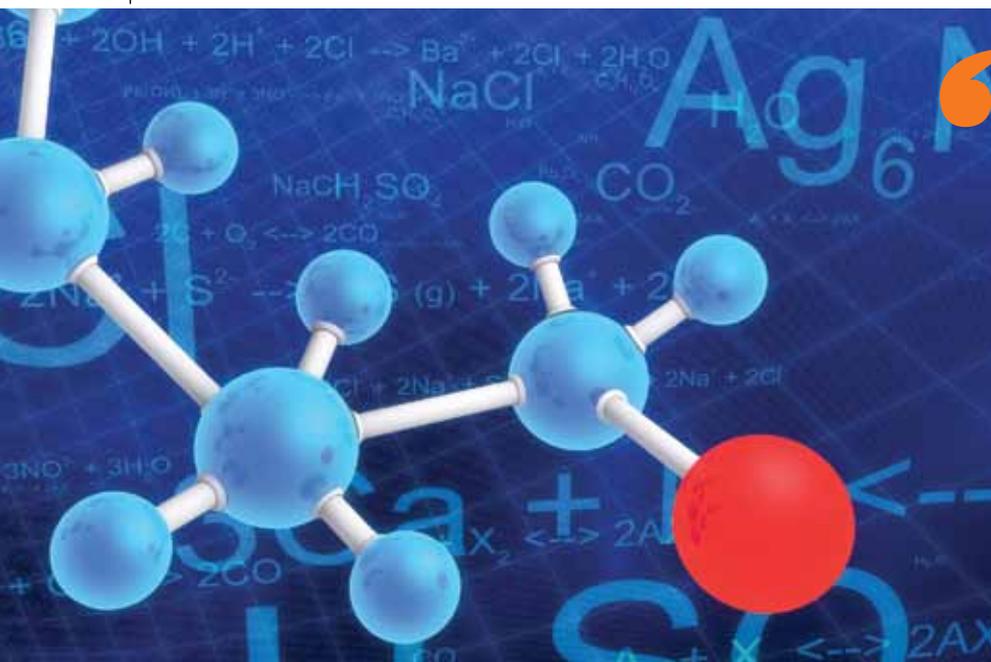
RECOMMENDATIONS

1. Up-level intelligence gathering and analysis
2. Activate smart monitoring
3. Reclaim access control
4. Get serious about effective user training
5. Manage the expectations of executive leadership
6. Rearchitect IT
7. Participate in information exchange

and systems—the “crown jewels”—in order to concentrate efforts on protecting these core assets. It also requires moving away from a perimeter-centric view. Focusing on fortifying the perimeter is a losing battle. Today’s organizations are inherently porous. Change the perspective to protecting data throughout its lifecycle across the enterprise and the entire supply chain.

Additionally, the definition of successful defense has to change from “keeping attackers out” to “sometimes attackers are going to get in; detect them as early as possible and minimize the damage.” Assume that your organization might already be compromised and go from there.

The following seven recommendations provide key ways to shore up defenses for organizations facing advanced persistent threats. It will take not only the commitment of the information-security team but also the support of executive leadership.

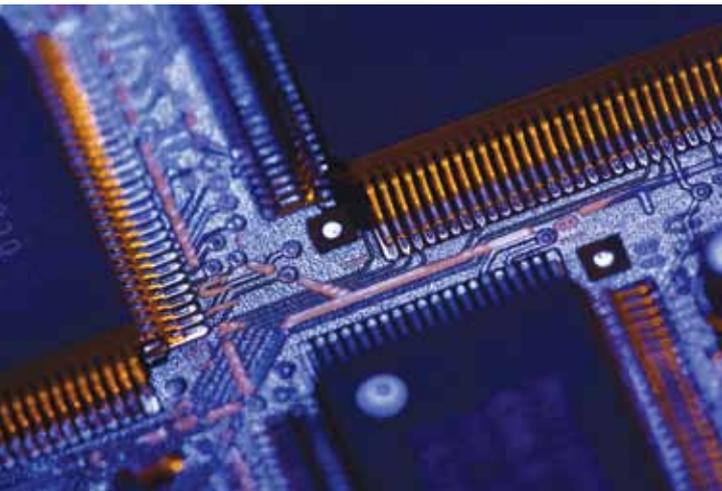


“It’s about the data. Security professionals have to start taking a data view of their organizations. It’s all around ‘Where is the data?’ and ‘Who is supposed to do what with it?’ which, in a huge corporation, is a huge challenge.”

MARENE N. ALLISON,
Worldwide Vice President of
Information Security,
Johnson & Johnson

CONVENTIONAL VS. ADVANCED APPROACHES TO INFORMATION SECURITY

	CONVENTIONAL APPROACH	ADVANCED APPROACH
CONTROLS COVERAGE	Protect all information assets	Focus protection efforts on most important assets (“crown jewels”)
CONTROLS FOCUS	Preventive controls (AV, firewall)	Detective controls (monitoring, data analytics)
PERSPECTIVE	Perimeter-based	Data-centric
GOAL OF LOGGING	Compliance reporting	Threat detection
INCIDENT MANAGEMENT	Piecemeal: find and neutralize malware or infected nodes	Big picture: find and dissect attack patterns
THREAT INTELLIGENCE	Collect information on malware	Develop deep understanding of attackers’ current targets and modus operandi and your own organization’s key assets and IT environment
SUCCESS DEFINED BY	No attackers get into the network	Attackers sometimes get in, but are detected as early as possible and impact is minimized



Recommendation 1. Up-level intelligence gathering and analysis

Many recent news reports have characterized the escalation of cyber attacks as cyber warfare. While this may be overly dramatic, it is true that organizations facing sophisticated threats are in a type of ongoing digital arms race. The adversaries have many weapons at their disposal and, in particular, they use knowledge against their targets. They know the organizations they are pursuing possibly better than the organizations themselves. This asymmetry gives them a huge advantage.

Deep knowledge about the threat landscape and about your own organization should be the cornerstone of your information-security strategy. Intelligence-gathering and analysis capabilities need to go beyond researching malware. Most organizations will need to take it to a new level in order to adequately evaluate the risks and devise strategies to mitigate them.

Must-have Intelligence on the Threats

What you should know about the threats includes:

- What digital assets are they going after?
- How do they pursue targets?
- What are their means, methods, motives?
- What actual attacks have occurred at other organizations?
- What do attack patterns look like?
- What does the malware look like?
- Are they planning attacks involving my industry?
- Is there chatter specifically about my organization being a target?

Use the answers to these questions in formulating your strategy—to determine, for example, the level of access controls on specific information, the type of background checks on personnel, and what events may be indications of compromise. By understanding the attackers’ techniques and plans, you’ll more likely detect an infiltration.

The challenge is that gathering intelligence costs money. Although a lot of threat information is available from publicly available sources (open source), it still requires skilled analysts to find, select, acquire, interpret, and communicate intelligence. To augment the security team’s capabilities, you can engage service providers such as intelligence-subscription services or consultants who can provide data on the threats.

There are also ways to participate in intelligence exchange, whereby organizations provide information about the threat activity they see in exchange for data from others. This will require spending time obtaining and preparing the information. Ultimately, organizations must recognize that intelligence has value and be prepared to invest dollars in collecting, purchasing, and/or exchanging the data. (To date, information exchange has not been that effective—see Recommendation 7.)

Required Knowledge of Internal Systems

Besides gaining intelligence on the threats, you should gain a detailed understanding of the digital assets within your organization that are potential targets. You must be able to answer the following questions:

- ➔ What are the most important digital assets to protect?
- ➔ Where are they located?
- ➔ Who has access to them?
- ➔ How are they protected?
- ➔ What is the state of existing security controls in relation to current attack tactics?
- ➔ Whose administrative privileges would it be most profitable for attackers to gain?
- ➔ Where are we most vulnerable?
- ➔ What does legitimate user activity look like throughout our environment?
- ➔ What constitutes normal network activity?
- ➔ Can we distinguish legitimate versus malicious activity?

Also use this internal intelligence to strengthen your strategy. Details about your most valuable digital assets show you where to focus your efforts,

“To detect ‘abnormal activity’ in your organization, networks, and systems, you should first understand and recognize ‘normal activity.’ Information-security departments should now invest in analyzing and interpreting day-to-day business flows and the marks they leave in existing detection systems.”

DR. MARTIJN DEKKER, Senior Vice President, Chief Information Security Officer, ABN Amro

“Know your enemy and know yourself and you can fight a thousand battles without disaster.”

From the “Art of War,” General Sun Wu Tzu (circa 500 BC)



such as what systems to ardently protect and what users to closely monitor. Given the shifting threat landscape, it may be necessary to re-evaluate what falls into scope—not only custodial data but also intellectual property, mission-critical systems, and so forth. This will have to be a cross-functional endeavor. You’ll need to work closely with the business-process owners and others across the organization to identify the most important data and systems. Creating an inventory of all high-value digital assets in a large global enterprise can be a huge challenge. Security teams may choose to deploy data-discovery tools and/or be able to leverage existing information from enterprise risk management (ERM) or governance, risk, and compliance (GRC) tools.

To detect anomalies which may indicate an attack, develop a baseline of normal activity. This will help pinpoint out-of-context data retrieval and unusual sequences of events. If there are certain events that make you suspicious and you can’t get internal confirmation, get an independent review.

Essential Information about Incidents

If data exfiltration is discovered, collect intelligence such as:

- ➔ Exactly what data did they take?
- ➔ Where was it sent?
- ➔ How long have the attackers been in our systems?
- ➔ Where did they go in the network?
- ➔ What rights did they have?
- ➔ Did they leave sleeper malware for back-door access down the road?

“The solution is to stop treating security as just a technology function. When you’re dealing with a highly sophisticated, deeply resourced adversary, you have to treat security as a counter-intelligence function.”

WILLIAM BONI, Vice President and Chief Information Security Officer, Corporate Information Security, T-Mobile USA

When dealing with advanced persistent threats, incident-response practices and forensic techniques should be designed to provide a high level of intelligence. In the face of compromise, it is important to understand the true nature of the incident and its scope. When data exfiltration is detected, the security team’s gut reaction will likely be to immediately shut it down. However, if possible, use the opportunity to observe where the traffic is going. Feed them false information and keep the channel open to gather more intelligence on the attack. Collecting intelligence at this point is extremely useful to your organization and others in defending against further attacks.

Recommendation 2. Activate smart monitoring

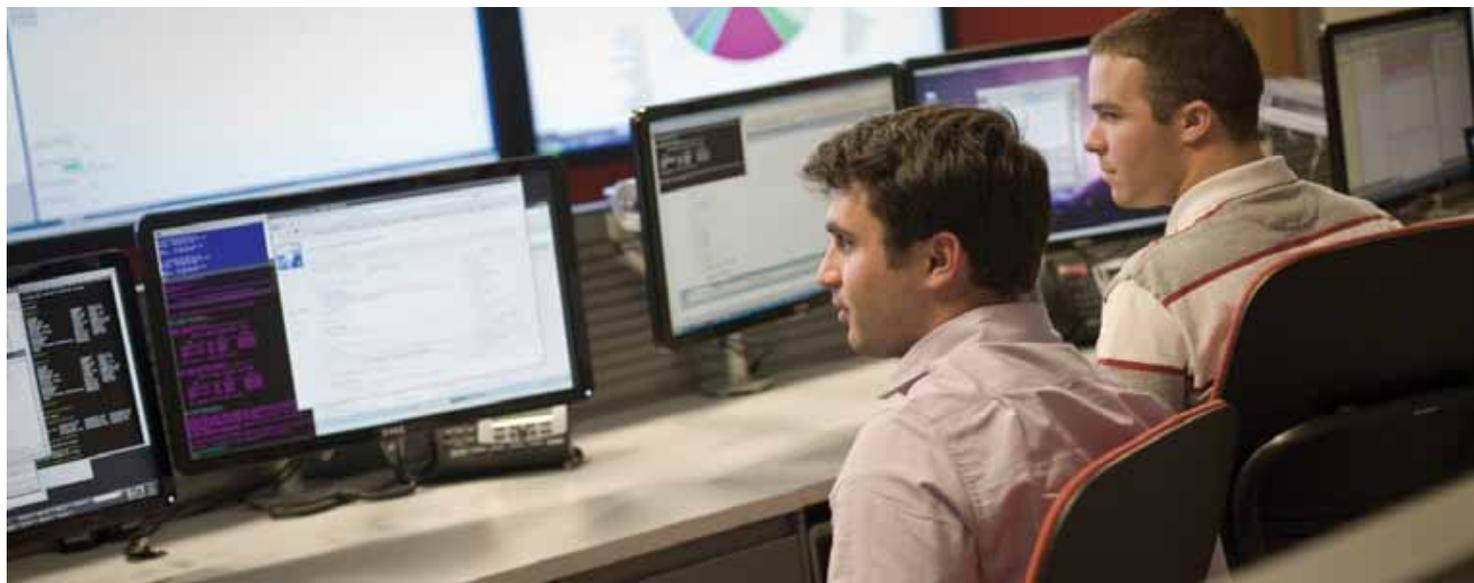
Forming a complete picture of malicious activities in the environment involves monitoring at multiple layers—application, host, network, and data—and the ability to associate events from multiple platforms. This is a tall order. The key is to inform your monitoring systems with a steady stream of current intelligence on the threats and your internal environment.

Over the past few years, organizations have implemented security information and event management (SIEM) infrastructure, with the objective of comprehensive monitoring. SIEM technology centralizes logs from many different

sources including firewalls, intrusion detection systems, Windows® servers, databases, web servers, and other types of applications and uses event correlation to detect incidents. Correlation of events that take place across the environment can be helpful for detecting complex attacks—that is, if you know the threats and your own assets. Often SIEM has been set up to meet compliance reporting requirements. To effectively use SIEM for threat detection, you need to know which data logs are relevant to capture and which events should be linked based on intelligence.

Security Data Analytics

Some security teams are pursuing even more powerful and in-depth analysis capabilities. An innovative approach to enterprise security is emerging based on using data analytics to detect malicious activity. These methods are modeled on “business-intelligence” systems that aggregate data, such as customer purchasing behavior, then use statistical analysis and data mining to identify business opportunities and inefficiencies. Similarly, data such as employee-access behavior can be aggregated then analyzed to discover security incidents. The concept is appealing: Use an analytical engine to sift through massive amounts of real-time and historical data at high speeds to develop trending on user and system activity and reveal anomalies that indicate compromise. One of the challenges will be storing and processing massive amounts of





The challenge with all-encompassing software-driven systems is they're great tools if you've got the management processes underneath them. Get organized first and build the processes you'll need to detect these sorts of attacks."

DAVID KENT, Vice President, Global Risk and Business Resources, Genzyme

data. As well, for meaningful analysis, you'll need to build effective analytical models. For detecting APTs in particular, the models will have to integrate knowledge of the threats.

The market is just beginning to offer some off-the-shelf solutions for systems like "security-data analytics" or "security-data warehouses." Some organizations are already developing their own home-grown system or piggy-backing off their existing business-intelligence platform. Besides technology, it's going to take people who can apply data analytics and business-intelligence skills to solve security problems. Forward-thinking security departments have already started building their own data-analytics teams or are working with existing teams from other parts of their organization. A source of people with this skill set is the banking industry, which employs data scientists who analyze data to detect financial fraud.

Visibility on the Network

Another important area of monitoring is looking at network traffic. One of the most common tools is an IDS. By monitoring packets in the network, an IDS looks for predetermined attack patterns (signatures) or abnormal traffic. For organizations with limited budget, there are open-source IDS tools available. A drawback with a conventional IDS is that a constantly updated library of signatures is needed. Organizations are dependent on the IDS vendors to develop and deploy signatures in a timely fashion. For APTs, since the attacks are not widely known, signatures are not widely available.

For detecting advanced attacks, some organizations have taken a different approach and deployed network-forensics tools that provide full packet capture and inspection capability. Network-forensics tools collect, process, and store all activities on the network. By interpreting network communications protocols (such as TCP, SQL, and so on), network-forensics technology recognizes activity as a transmission, database transaction, data element, and so forth and reports on every single activity that occurs. Based on threat intelligence, the complete dataset of network activity can then be queried on indicators such as known techniques, identifiers, and addresses. For example, you may have an IP address identifying a command-and-control site and query on, "Show me anywhere one of my systems is communicating with this IP address within this application." You may know information on a tactic and ask, "Show me anywhere executable code is traversing my infrastructure." As your understanding of the threat and the threat actors evolves, you can go back and refine your analysis.

If the threat information can be represented as structured data such as lists of IP addresses, domain names, user names, file names, transaction types, keywords, and so forth, threat intelligence can be fed directly into the system for automatic analysis of network activity. Sources include community Internet threat-intelligence services, commercial threat-intelligence feeds, US-CERT, NSA, or external/internal threat intelligence the organization has produced itself.

One of the challenges with network-forensics technology is that recording every single event on the network generates massive amounts of data. It will take resources to store and process it. You will also need people on your team who know how to analyze



it in a way that derives meaning. They will have to be able to take intelligence and translate it into useful queries and/or data for automated detection. These are new skills that only a few organizations currently have.

Overall, with new approaches to monitoring, it will be necessary to rethink what an incident is and how to construct an incident-response process, especially given that some organizations will be in a continual state of compromise. Next-generation incident monitoring changes the type of people and positions that will be needed in your Security Operations Center (SOC) or Computer Incident Response Team (CIRT). As well, be aware that being in a constant state of compromise can overtax your security team. Take the lead from organizations in the defense industries and work towards developing a “battle rhythm” for combating APTs.

Although the focus for detecting APTs is often new approaches to monitoring, being even more diligent about existing security mechanisms cannot be overlooked. For example, configuration management and patch management are two areas that need attention. Systems must be monitored to ensure they are properly configured and have up-to-date settings and protections. Many attacks exploit poorly configured or unpatched systems. Moving to more automation in these areas can help reduce the burden on IT and security staff and free them up to focus on building new competencies.

Recommendation 3. Reclaim access control

A key defensive measure is to make it harder for the attackers to obtain access rights. To begin with, tighten up least-privilege policy. For critical assets, re-evaluate who absolutely needs access and, as much as possible, reduce the number of people who have it.

The most sought-after credentials are privileged users. Put in place strict controls on administrative access. This may require controlling the way administrators work, which will likely meet with a



“FOR IDENTITY management, don’t tackle the whole company. Tackle the highest domain-level privileges first, because that’s where they’re going to go first—I think we’ve got plenty of evidence of that. Identity is a critical area and a key component of defense in depth. Unfortunately it is often overlooked because it is challenging to tackle.”

TIMOTHY MCKNIGHT, Vice President and Chief Information Security Officer, Northrop Grumman

lot of resistance because it will decrease convenience. You’ll need to work closely with IT as well as the business-process owners and asset owners to drive support for measures such as:

- Only allow your administrators to log in to their administrator accounts on specific boxes
- Do not allow remote access, email, web surfing, and so forth on these boxes
- Require face-to-face password changes and/or multi-factor authentication for administrator accounts
- End the use of administrative passwords that work across the whole system
- Reduce the number of people who have administrative rights that allow them to roam the network
- Use ways to separate the administrator group from the general user population (for example jump servers)
- Perform extensive monitoring on all administrative users

By eliminating passwords, you can eliminate attackers’ ability to exploit accounts by obtaining or cracking passwords. Some organizations are moving their entire user population to multi-factor authentication in order to combat advanced persistent threats.



You have to be on high alert for high-value compromises now, especially any events involving administrative users. Don’t assume it’s just an admin error. Get confirmation.”

RENEE GUTTMANN, Chief Information Security Officer,
The Coca-Cola Company



If you do it proactively and keep educating your user population, I think they will—over time—understand how to make a distinction between what is real mail and what is phishing mail. If you use statistical information to see what training strategies really work, your strategies should get more mature.”

VISHAL SALVI, Chief Information Security Officer and Senior Vice President, HDFC Bank Limited

Recommendation 4. Get serious about effective user training

No matter what security technologies are implemented, every organization’s greatest vulnerability is its people. Social engineering is a predominant aspect of advanced persistent attacks—finding ways to increase the effectiveness of user training has become imperative. Traditional user-training methods such as web courses, videos, and classroom presentations don’t involve the user in active defense. Training mechanisms should make the threat real for the individual user, engage them in actively defending the organization, and drive home the message that users could be personally responsible for a major information breach.

A novel educational approach is based on conducting simulated phishing and spear-phishing attacks on groups of users to give them real-life experience and test their responses. Some organizations are developing phishing tests internally and others are using automated phishing-diagnostic tools, which are now available. The automated tools help educate users to recognize phishing exploits by providing real-time feedback. If a user succumbs to the test’s false messages, the user is immediately notified and told what he/she did wrong. The security team can adjust its education program to keep up with evolving tactics. As new styles of attack arise, the team can send out new phishing messages that incorporate these new methods to see how employees react. The tools also help to measure results over time by providing statistics on how many users click on messages. Of course, it will be essential for the security team to work closely with other departments such as Human Resources in conducting these tests.

Another active training technique is the use of Serious Gaming. With this method, employees play a computer game within a virtual environment that simulates their own workspace. The employee is put through various typical real-life situations unique to their job, including a fully simulated social-engineering attack. The employee is aware that it is a game, but must respond the same way they would in their everyday work experience. It helps users to see how real the threat is and that they could be personally responsible for exposing the organization. Evaluating how users respond to the game can help the security team assess and adapt the security program.

A crucial component of more effective training is getting users to recognize their responsibility. In this respect, traditional training programs have been tepid at best. The severity of the threat and the potentially profound personal culpability users could face has not been effectively communicated. Every employee should be made to realize that by clicking on an email they could be personally responsible for enabling an attacker to steal the most highly valued digital assets, potentially devastating the entire organization. This requires a cultural change and a more disciplinary approach to security.

For example, if a user is spear-phished because they didn’t take adequate precautions, perhaps they should have to face disciplinary consequences. In some organizations this will be met with resistance because it may scare users. But given the escalating threat landscape, it may take scaring users for them to recognize the reality of the threat and give them reason to care personally about security. For this cultural change to occur, the executive leadership has to understand the need for it and be supportive.

While increasing users’ awareness of the threats and making them take more responsibility for security is absolutely necessary, it’s important to recognize that it will not be 100 percent successful. When it comes to social engineering, the perpetrators are masters of disguise. Their emails, messages, or phone calls can seem entirely legitimate. Even security people could fall for them.

Recommendation 5. Manage the expectations of executive leadership

It is a common mantra in information security that you need awareness and buy-in from the top. In the current landscape, you won't survive without it. Given the news reports, the executive team and board of directors will likely be aware of escalating threats, but not appreciate the true extent of the risks and realize what it will take to combat them. Making the business case for the people, process, and/or technology the security team requires could be challenging, especially since cyber threats are still a vague concept for many executives. One way to help get the message across is to present case studies on real incidents at other companies including the financial and business impact. Another way is to leverage government agencies. Have them brief your executives on current threats and tactics to help the C-suite understand the serious nature of these threats.

Your communications plan for executive leadership should help shape their perceptions and expectations. The C-suite may perceive security to be similar to other challenges they face: With the right investments, it can be fixed. Or they may see security as a compliance issue: If the check boxes are completed, it's done. Instead, help them see that advanced persistent threats are not going to be solved. Combating them involves fighting an ongoing digital arms race, continually assessing threats and modifying security strategies. Investing in security won't stop attacks from happening. But with adequate resources, the organization will be able to

keep pace with the digital arms race, manage the risks, and—when the inevitable attack occurs—be able to minimize the damage. Convey this reality to executive leadership and infuse your message with threat intelligence.

Gain support for an organizational structure that can contend with advanced persistent threats. The threat actors are extremely clever in forming multi-disciplinary teams. To be ready to defend against them, the enterprise will need to be well-organized. The security team should drive executive support for cross-functional teams and/or steering committees, which can bring together different skills and expertise and coordinate efforts.

To succeed in rallying support from executives, you'll have to put information-security investments in context. Demonstrate that you're making effective use of investments through metrics and benchmarking. Recognize that at the executive level, information-security risk is just one of a whole portfolio of risks the enterprise faces such as financial risks or market risks. Therefore, describe the probability and impact of APTs and help executives weigh this risk versus other types of risk. Information risk management should be integrated into the overall enterprise risk-management strategy.

"IT IS most worrying to meet a board director who asks the blunt question 'Are we secure —yes or no?' What you want them to show is a better understanding of risk management and ask, 'Are you getting enough support and funding for your security capability so that you can keep up with this digital arms race?'"

PROFESSOR PAUL DOREY, Founder and Director, CSO Confidential and Former Chief Information Security Officer, BP





"BEING ABLE to justify the technological improvements, the intelligence and monitoring capabilities, the continual refresh—which is what you need for protecting networks—would be much easier for entities that provided IT services and held the liability for protecting those networks."

MISCHEL KWON, Former Director, U.S. Computer Emergency Readiness Team (CERT); President, Mischel Kwon & Associates

Recommendation 6. Rearchitect IT

Combatting APTs will require not only different approaches in security but also changes in IT. To address a major weakness, many organizations will need to rethink network design. Flat networks make it easy for cyber criminals to freely move around and find the data they're after through any machine on the network. Instead of flat networks, organizations should set up network zones to isolate critical assets and compartmentalize the network environment. Depending on the value or sensitivity of information assets, consider taking certain data off the network altogether.

Desktop virtualization and thin computing can also help in rearchitecting systems to be more secure. With these technologies, digital assets are less accessible to attackers, since data is stored on a centralized server and viewed over the network but not downloadable or transferable.

To reduce the number of vulnerabilities in applications, organizations should commit to effective software-assurance methods. For in-house development, implement standards for software development lifecycle (SDLC) including robust security. For off-the-shelf solutions, ensure that your vendors follow industry best practices for developing and delivering more secure and reliable software, hardware, and services.

Keeping pace with advanced persistent threats requires a continual upgrade of people, process, and technology over time. This could become expensive for some organizations. For organizations without the requisite resources and expertise, a possible solution is to move to IT service providers

which have the ability to stay on the cutting edge of intelligence gathering and information security. If a company's sole mission is to provide secure IT infrastructure—and whose bottom line and stock price depend on it—they may be more incentivized to make the necessary investments. Contracting out to IT experts to run a secure IT infrastructure may also be cost-efficient because the costs would be shared across multiple customer organizations. This is a ripe opportunity for cloud computing. Realizing this promise will depend on cloud providers' ability to step up to the plate and deliver cost-effective IT services with reliable, robust, and scalable security.



Recommendation 7. Participate in information exchange

Ultimately, defending against advanced persistent threats will take not only new models for enterprise IT but also new models for information sharing. Current channels for information sharing include, for example, the Information Sharing and Analysis Centers (ISACs) in North America. However, the existing channels can be too slow in disseminating threat information. The life span of the typical attack signature is measured in hours; once the attackers detect that it's been shared, they immediately stop using it. Sharing mechanisms need to be more real-time so that once a signature is identified, it can be disseminated to other organizations while it's still useful to detect attacks.

Another major problem is that industry and government are very reluctant to share threat information for various reasons, especially perceived legal risks. Since the vast majority of critical infrastructure is owned by private entities, there needs to be more broad-based participation in intelligence exchange, including in the financial-services, energy, utilities, telecom, and technology sectors. Often in information exchanges, many

organizations would like to receive threat intelligence but few organizations have much willingness to contribute. To fix this, there has to be an incentive for organizations to collaborate.

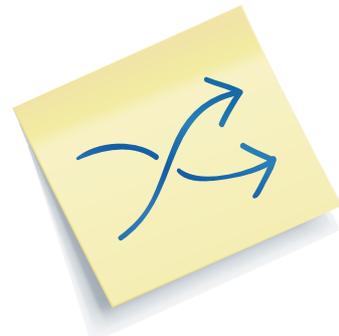
Some believe that the current impasse in information sharing has reached the point where it requires legislation. Not legislation that would set up a government-led coordination effort; this is likely not the answer. But a more valuable role for government might be to remove the impediments to information sharing. Specifically, legislation could address the liability issues that concern so many corporate legal departments. As well, the government could legislate that if a company is of a certain size or part of critical infrastructure then it must belong to a trust community. A workable model would have to ensure that participation would be anonymous so that no information could be traced back to a specific entity.

A critical step would be for organizations to start working more with law enforcement. In many instances when an organization is compromised, they do not report the incident. Yet agencies such as the FBI and NSA (in the U.S.) need the information in their collection of evidence against cyber criminals and have threat information which may help the organization defend against further attacks.



“It’s the real conundrum of information sharing—how do you share information that needs to be tightly held with the broadest amount of people in the shortest amount of time in a form that they can immediately consume?”

DAVE MARTIN, Chief Security Officer, EMC Corporation



5

Conclusion



With the number of APT-style attacks on the rise, targeting government and industry across the globe, it is clear that most organizations are now facing a whole new category of threat. At the same time, inherent weaknesses in enterprise IT and ineffective approaches to information security are putting organizations at risk. There is a growing realization that confronting advanced persistent threats calls for a whole new doctrine of defense.

Keeping pace with the digital arms race requires constantly re-evaluating your position against the threats and adapting your information-security strategies. Intelligence gathering has become an essential core competency for every security team. For many organizations, contending with APTs will also demand cultural changes. The information-security strategies must take into account that no organization is impenetrable and instead focus on protecting

what matters most. The executive leadership must make a commitment to an ongoing effort and the general user population has to take on real responsibilities for information security.

To combat advanced persistent threats, government agencies and corporations must work to overcome their current reluctance to share information and build communities of trust. In today's threat landscape, an organization cannot sit in isolation and expect to be able to defend itself. Global organizations need to participate on a national and even international scale. The result would bring benefits for individual organizations as well as improve security overall for public and private sectors.

"WITH ADVANCED persistent threats, we have to start shifting our way of thinking from the fortress model of security strategies. We have to be able to not only prevent-detect-respond, but also live continuously in a compromised situation and still run operations."

FELIX MOHAN, Chief Security Officer, Airtel



About the Security for Business Innovation Council Initiative

Business innovation has reached the top of the agenda at most enterprises, as the C-suite strives to harness the power of globalization and technology to create new value and efficiencies. Yet there is still a missing link. Though business innovation is powered by information and IT systems, protecting information and IT systems is typically not considered strategic—even as enterprises face mounting regulatory pressures and escalating threats. In fact, information security is often an afterthought, tacked on at the end of a project or—even worse—not addressed at all. But without the right security strategy, business innovation could easily be stifled or put the organization at great risk.

AT RSA, WE BELIEVE THAT IF SECURITY TEAMS are true partners in the business-innovation process, they can help their organizations achieve unprecedented results. The time is ripe for a new approach; security must graduate from a technical specialty to a business strategy. While most security teams have recognized the need to better align security with business, many still struggle to translate this understanding into concrete plans of action. They know where they need to go, but are unsure how to get there. This is why RSA is working with some of the top security leaders in the world to drive an industry conversation to identify a way forward.

RSA HAS CONVENED A GROUP OF HIGHLY successful security executives from Global 1000 enterprises in a variety of industries which we call the “Security for Business Innovation Council.” We are conducting a series of in-depth interviews with the Council, publishing their ideas in a series of reports, and sponsoring independent research that explores this topic. RSA invites you to join the conversation. Go to www.rsa.com/securityforinnovation to view the reports or access the research. Provide comments on the reports and contribute your own ideas. Together we can accelerate this critical industry transformation.

Security for Business Innovation Report Series

GO TO WWW.RSA.COM/securityforinnovation

THE TIME IS NOW:
Making Information Security Strategic to Business Innovation

MASTERING THE RISK/
REWARD EQUATION:
Optimizing Information Risks to Maximize Business Innovation Rewards

DRIVING FAST AND FORWARD:
Managing Information Security for Strategic Advantage in a Tough Economy

CHARTING THE PATH:
Enabling the “Hyper-Extended” Enterprise in the Face of Unprecedented Risk

BRIDGING THE CISO-CEO DIVIDE

THE RISE OF USER-DRIVEN IT:
Re-calibrating Information Security for Choice Computing

THE NEW ERA OF COMPLIANCE: Raising the Bar for Organizations Worldwide

BUSINESS INNOVATION DEFINED

Enterprise strategies to enter new markets, launch new products or services, create new business models, establish new channels or partnerships, or transform operations



Contributors

Top information-security leaders from Global 1000 enterprises



MARENE N. ALLISON, Worldwide Vice President of Information Security, **JOHNSON & JOHNSON**

Prior to joining Johnson & Johnson, Marene was a senior security executive at Medco, Avaya, and the Great Atlantic and Pacific Tea Company. She served in the United States Army as a military police officer and as a special agent in the FBI. Marene is on the board of directors of the American Society of Industrial Security International (ASIS) and the Domestic Security Alliance Council (DSAC) and is President of West Point Women. She is a graduate of the U.S. Military Academy.



ANISH BHIMANI, CISSP, Chief Information Risk Officer, **JPMORGAN CHASE**

Anish has global responsibility for ensuring the security and resiliency of JPMorgan Chase's IT infrastructure and supports the firm's Corporate Risk Management program. Previously, he held senior roles at Booz Allen Hamilton, Global Integrity Corporation, and Predictive Systems. Anish was selected "Information Security Executive of the Year for 2008" by the Executive Alliance and named to Bank Technology News' "Top Innovators of 2008" list. He authored "Internet Security for Business" and is a graduate of Brown and Carnegie-Mellon Universities.



WILLIAM BONI, CISM, CPP, CISA, Vice President and Chief Information Security Officer, **T-MOBILE USA**

An information-protection specialist for 30 years, Bill joined T-Mobile in 2009. Previously, he was Corporate Security Officer of Motorola Asset Protection Services. Throughout his career, Bill has helped organizations design and implement cost-effective programs to protect both tangible and intangible assets. He pioneered the application of computer forensics and intrusion detection to deal with incidents directed against electronic business systems. Bill was awarded CSO Magazine's "Compass Award" and "Information Security Executive of the Year - Central" in 2007.



ROLAND CLOUTIER, Vice President, Chief Security Officer, **AUTOMATIC DATA PROCESSING, INC.**

Roland has functional and operational responsibility for ADP's information, risk, crisis-management, and investigative-security operations worldwide. Previously, he was CSO at EMC and held executive positions with consulting and managed-services firms. He has significant experience in government and law-enforcement, having served in the U.S. Air Force during the Gulf War and later in federal law-enforcement agencies. Roland is a member of the High Tech Crime Investigations Association, the State Department Partnership for Critical Infrastructure Security, and Infragard.



DAVID KENT, Vice President, Global Risk and Business Resources, **GENZYME**

David is responsible for the design and management of Genzyme's business-aligned global security program, which provides Physical, Information, IT, and Product Security along with Business Continuity and Crisis Management. Previously, he was with Bolt Beranek and Newman Inc. David has 25 years of experience aligning security with business goals. He received CSO Magazine's 2006 "Compass Award" for visionary leadership in the Security Field. David holds a Master's degree in Management and a Bachelor of Science in Criminal Justice.



PETRI KUIVALA, Chief Information Security Officer, **NOKIA**

Petri has been CISO at Nokia since 2009. Previously, he led Corporate Security operations globally and prior to that in China. Since joining Nokia in 2001, he has also worked for Nokia's IT Application Development organization and on the Nokia Siemens Networks merger project. Before Nokia, Petri worked with the Helsinki Police department beginning in 1992 and was a founding member of the Helsinki Criminal Police IT-investigation department. He holds a degree in Master's of Law.



DAVE MARTIN, CISSP, Chief Security Officer, **EMC CORPORATION**

Dave is responsible for managing EMC's industry-leading Global Security Organization (GSO) focused on protecting the company's multibillion-dollar assets and revenue. Previously, he led EMC's Office of Information Security, responsible for protecting the global digital enterprise. Prior to joining EMC in 2004, Dave built and led security-consulting organizations focused on critical infrastructure, technology, banking, and healthcare verticals. He holds a B.S. in Manufacturing Systems Engineering from the University of Hertfordshire in the U.K.



TIMOTHY MCKNIGHT, CISSP, Vice President and Chief Information Security Officer, **NORTHROP GRUMMAN**

Tim is responsible for Northrop Grumman's cyber-security strategy and vision, defining company-wide policies and delivering security to support the company. Tim received the Information Security Executive of the Year Mid-Atlantic Award and Information Security Magazine Security 7 Award in 2007. Tim has held management roles with BAE and Cisco Systems and served with the FBI. He has a Bachelor's degree and completed Executive Leadership training at the Wharton School. Tim also served as adjunct faculty at Georgetown University.



GUEST CONTRIBUTOR

MISCHEL KWON,

Former Director, U.S. Computer Emergency Readiness Team (CERT); President, **MISCHEL KWON & ASSOCIATES**

Mischel leads a security-consulting firm specializing in Technical Defensive Security, Security Operations, and Information Assurance. Previously, she served as VP of Public Sector Security at RSA, The Security Division of EMC; Director of U.S.- CERT; and Deputy Director for IT Security Staff at the Department of Justice (DOJ). Mischel has a M.Sc. in Computer Science and a graduate certificate in Computer Security and Information Assurance and is an adjunct professor at George Washington University.



DAVE CULLINANE,

Chief Information Security Officer and Vice President, Global Fraud, Risk & Security, **EBAY**

Dave has more than 30 years of security experience. Prior to joining eBay, Dave was the CISO for Washington Mutual and held leadership positions in security at nCipher, Sun Life, and Digital Equipment Corporation. Dave is involved with many industry associations including as current Past International President of ISSA. He has numerous awards including SC Magazine's Global Award as CSO of the Year for 2005 and CSO Magazine's 2006 Compass Award as a "Visionary Leader of the Security Profession."



DR. MARTIJN DEKKER, Senior Vice President, Chief Information Security Officer, **ABN AMRO**

Martijn was appointed Chief Information Security Officer of ABN Amro in early 2010. Previously he held several positions in information security and IT including Head of Information Security and Head of Technology Risk Management in the Netherlands. Other positions included IT Architect, Program/Portfolio Manager, and IT Outsourcing/Offshoring Specialist. Martijn joined ABN Amro in 1997 after completing his Ph.D. in Mathematics at the University of Amsterdam and a Master's of Mathematics at the University of Utrecht.



PROFESSOR PAUL DOREY, Founder and Director, CSO Confidential and Former Chief Information Security Officer, **BP**

Paul is engaged in consultancy, training, and research to help vendors, end-user companies, and governments in developing their security strategies. Before founding CSO Confidential, Paul was responsible for IT Security and Information and Records Management at BP. Previously, he ran security and risk management at Morgan Grenfell and Barclays Bank. Paul was a founder of the Jericho Forum, is Chairman of the Institute of Information Security Professionals, and a Visiting Professor at Royal Holloway College, University of London.



RENEE GUTTMANN, Chief Information Security Officer, **THE COCA-COLA COMPANY**

Renee is responsible for the information-risk-management program at The Coca-Cola Company. Previously, she was VP of Information Security and Privacy at Time Warner and Senior Director of Information Security at Time Inc. She has also held information-security roles at Capital One and Glaxo Wellcome and has been a security analyst at Gartner. Renee received the 2008 Compass Award from CSO Magazine and in 2007 was named a "Woman of Influence" by the Executive Women's Forum.



FELIX MOHAN, Chief Security Officer, **AIRTEL**

At Airtel, Felix ensures that information security and IT align with changes to the risk environment and business needs. Previously, he was CEO at a security-consulting firm, an advisor with a Big-4 consulting firm, and head of IT and security in the Indian Navy. He was a member of India's National Task Force on Information Security, Co-chair of the Indo-U.S. Cybersecurity Forum, and awarded the Vishisht Seva Medal by the President of India for innovative work in Information Security.



RALPH SALOMON, Vice President, IT Security & Risk Office, Global IT, **SAP AG**

Ralph is responsible for developing and maintaining the global IT security strategy and operational IT security at SAP worldwide. His many accomplishments include integration of Security, Quality, and Risk Management and improvements in IT Service and Business Continuity Management, which led SAP to achieve ISO 27001 certification and to become the first German company to be BS25999 certified. Prior to SAP, Ralph worked at KPMG as an IT Security, Quality, and Risk Management advisor and auditor.



VISHAL SALVI, CISM Chief Information Security Officer and Senior Vice President, **HDFC BANK LIMITED**

Vishal is responsible for driving the Information-Security strategy and its implementation across HDFC Bank and its subsidiaries. Prior to HDFC, he headed Global Operational Information Security for Standard Chartered Bank (SCB) where he also worked in IT Service Delivery, Governance, and Risk Management. Previously, Vishal worked at Crompton Greaves, Development Credit Bank, and Global Trust Bank. He holds a Bachelor's of Engineering degree in Computers and a Master's in Business Administration in Finance from NMIMS University.



DENISE WOOD, Chief Information Security Officer and Corporate Vice President, **FEDEX CORPORATION**

Denise is responsible for security and business-continuity strategies, processes, and technologies that secure FedEx as a trusted business partner. Since joining in 1984 she has held several Information Technology officer positions supporting key corporate initiatives, including development of fedex.com, and was the first Chief Information Officer for FedEx Asia Pacific in 1995. Prior to FedEx, Denise worked for Bell South, AT&T, and U.S. West. Denise was a recipient of Computerworld's "Premier 100 IT Leaders for 2007" award.



Quotable *Highlights from the conversation*

Marene N. Allison, Worldwide Vice President of Information Security, Johnson & Johnson

"IT'S ABOUT the data. Security professionals have to start taking a data view of their organizations. It's all around 'Where is the data?' and 'Who is supposed to do what with it?' which, in a huge corporation, is a huge challenge."

William Boni, Vice President and Chief Information Security Officer, Corporate Information Security, T-Mobile USA

"THE SOLUTION is to stop treating security as just a technology function. When you're dealing with a highly sophisticated, deeply resourced adversary, you have to treat security as a counter-intelligence function."

Roland Cloutier, Vice President, Chief Security Officer, Automatic Data Processing, Inc.

"IT IS a very intelligent, well-armed, and effective foe that is fantastic at what they do, and it's going to take a new approach in most enterprises to combat it."

Dave Cullinane, Chief Information Security Officer and Vice President, Global Fraud, Risk & Security, eBay

"THE FACT is there is very sophisticated, stealthy stuff running out there. So unless you're looking for the right things, like connections out to the Internet, you're not going to see this stuff."

Dr. Martijn Dekker, Senior Vice President, Chief Information Security Officer, ABN Amro

"ADVANCED PERSISTENT threats in the banking industry combine knowledge of malware with, for example, clever social engineering and a deep understanding of banking. Advanced persistent threats have a high degree of organization bringing together different people with different skills."

"TO DETECT 'abnormal activity' in your organization, networks, and systems, you should first understand and recognize 'normal activity.' Information-security departments should now invest in analyzing and interpreting day-to-day business flows and the marks they leave in existing detection systems."

Professor Paul Dorey, Founder and Director, CSO Confidential and Former Chief Information Security Officer, BP

"IT IS most worrying to meet a board director who asks the blunt question 'Are we secure—yes or no?' What you want them to show is a better understanding of risk management and ask, 'Are you getting enough support and funding for your security capability so that you can keep up with this digital arms race?'"

Renee Guttman, Chief Information Security Officer, The Coca-Cola Company

"YOU HAVE to be on high alert for high-value compromises now, especially any events involving administrative users. Don't assume it's just an admin error. Get confirmation."

David Kent, Vice President, Global Risk and Business Resources, Genzyme

"THE CHALLENGE with all-encompassing software-driven systems is they're great tools if you've got the management processes underneath them. Get organized first and build the processes you'll need to detect these sorts of attacks."

Petri Kuivala, Chief Information Security Officer, Nokia

"FIRST OF ALL, classify your assets extremely well so that you understand what must be protected from a confidentiality point of view. Then you plan protection for those systems much more carefully than you would for some other systems."



Quotable *Highlights from the conversation*

Mischel Kwon, Former Director, U.S. Computer Emergency Readiness Team (CERT); President, Mischel Kwon & Associates

"BEING ABLE to justify the technological improvements, the intelligence and monitoring capabilities, the continual refresh—which is what you need for protecting networks—would be much easier for entities that provided IT services and held the liability for protecting those networks."

Timothy McKnight, Vice President and Chief Information Security Officer, Northrop Grumman

"FOR IDENTITY management, don't tackle the whole company. Tackle the highest domain-level privileges first, because that's where they're going to go first—I think we've got plenty of evidence of that. Identity is a critical area and a key component of defense in depth. Unfortunately it is often overlooked because it is challenging to tackle."

Dave Martin, Chief Security Officer, EMC Corporation

"IT'S THE real conundrum of information sharing—how do you share information that needs to be tightly held with the broadest amount of people in the shortest amount of time in a form that they can immediately consume?"

Felix Mohan, Chief Security Officer, Airtel

"WITH ADVANCED persistent threats, we have to start shifting our way of thinking from the fortress model of security strategies. We have to be able to not only prevent-detect-respond, but also live continuously in a compromised situation and still run operations."

Vishal Salvi, Chief Information Security Officer and Senior Vice President, HDFC Bank Limited

"IF YOU do it proactively and keep educating your user population, I think they will—over time—understand how to make a distinction between what is real mail and what is phishing mail. If you use statistical information to see what training strategies really work, your strategies should get more mature."

Ralph Salomon,

Vice President, IT Security & Risk Office, Global IT, SAP AG

"THE GERMAN Federal Office for Protection of the Constitution and the Federal Criminal Police Office have confirmed in their reports that there is increased activity regarding targeted, sophisticated attacks. These are coming from foreign countries' agencies but also some criminal organizations are trying to get hold of IP from different companies."

Denise Wood, Chief Information Security Officer and Corporate Vice President, FedEx Corporation

"IF THE threat actors who have gone looking for zero-day vulnerabilities decide to monetize all the zero-day vulnerabilities they're stockpiling, that might be an issue."

DATA

