

Synopsis of the 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



This synopsis is a small teaser of the wealth of information provided by the Security for Business Innovation Council. For a deeper dive, please view the full report at www.rsa.com/securityforinnovation.



The Shifting Threat Landscape

"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.



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, these incidents have pushed "APT" into the mainstream.

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 custodial data like credit card numbers, APTs focus on obtaining high-value digital assets or tapping into critical systems.

This eighth report from the Security for Business Innovation Council (SBIC) examines what has changed in the threat landscape, discusses why enterprises are vulnerable, and offers 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.

Key Features of APTs

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

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

² *Growing Risk of Advanced Threats*, Ponemon Institute, June 30, 2010

Signs of a Growing Menace

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. National-security agencies around the globe have been tracking an increase in sophisticated threats and communicating their findings to industry.¹ Recent research by the Ponemon Institute also shows an escalation of threats.²

Several factors are driving this escalation. The global economy has become fiercely competitive and some players are resorting to illegal methods to gain the upper hand. 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.

And it's no longer just a few countries that have APT capabilities. Beyond nation-states, other threat actors such as organized crime and even politically motivated "hacktivists" are also using similar techniques.





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

Inherent Weaknesses in IT

As organizations expand, merge, and develop global supply chains, they combine new and legacy systems, link networks, and integrate with third-party service providers. The complexity of enterprise IT 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 creating new attack vectors.

Another weakness is flat network design. While having one broadcast domain costs less and is more flexible than highly segregated networks, it facilitates attackers' ability to roam the network and possibly reach high-value systems.

Application vulnerabilities also predispose enterprises to attacks. Many standard business applications were developed over years and contain millions of lines of code, making security holes inevitable. Also, applications often are not built securely from the outset or are outliving the security of their components, creating more vulnerabilities for threat actors to exploit.

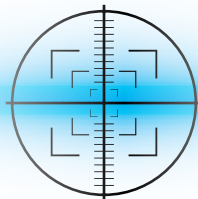
Ineffective Approaches to Information Security

Adding to the problem is that many security teams are not able to detect sophisticated attack patterns. While conventional tools might identify an unauthorized access, a virus, a phishing e-mail, or a piece of malware, they 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. APTs attack from multiple directions, combining 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.





Recommendations

"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



It will take new ways of thinking about information security to combat this new class of threat. For example, tackling APTs means giving up the idea that it is possible to protect everything. Security teams will have to work closely with the business to identify the most critical information and systems in order to concentrate on protecting these core assets. The Council report offers a set of concrete recommendations for organizations facing APTs to shore up their defenses. Specific guidance and "how to" strategies include:

1. **Up-level intelligence gathering and analysis:** Make intelligence the cornerstone of your strategy.
2. **Activate smart monitoring:** Use intelligence to inform your monitoring and track user behavior and network traffic to form an aggregated picture of malicious activities.
3. **Reclaim access control:** Tighten up least-privilege policy, create strict controls on administrative access, and move towards multi-factor authentication.
4. **Get serious about effective user training:** Train your users to recognize social engineering and compel them to take responsibility for organizational security.
5. **Manage the expectations of executive leadership:** Help executives understand that successful security no longer means keeping attackers out but rather detecting them as early as possible and minimizing the damage.
6. **Rearchitect IT:** Move from flat to segregated networks so it's harder for attackers to roam the network and find your key assets.
7. **Participate in intelligence exchange:** Leverage knowledge from other organizations by sharing threat intelligence.

THE SECURITY FOR BUSINESS INNOVATION 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, protecting information 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 the organization could be put 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 top security leaders from around the world to drive an industry conversation and chart the way forward.

Conclusion

There is a growing realization that confronting APTs calls for a 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. Contending with APTs will likely also demand cultural changes. Information-security strategies must acknowledge that no organization is impenetrable and instead focus on protecting what matters most. Executive leadership must make a commitment to ongoing effort and the user population has to take on real responsibility. Finally, government agencies and corporations must overcome their reluctance to share information and build communities of trust in order to improve security overall for public and private sectors.

