WHITE PAPER

# Evolving Uses of Technology: Mobility and Cybersecurity

***March 2012***

*Conventional security standards and practices cannot keep up with the frequency and sophistication of attacks.*

## EXECUTIVE SUMMARY

Mobility. Virtualization. The smartphone. Tablets. Telecommuting and remote access. Technology advancements, device innovation and the ability to connect to just about anyone or anything from almost anywhere has fundamentally changed the way we communicate and how business gets done.

And there's no looking back. Instead, dependence on these technologies and the networks that provide critical support has increased, not just for colleague-to-colleague interaction, but also for access to applications and data in private and public clouds. E-commerce, social media companies and revenue streams based on flowing media to audiences around the globe simply wouldn't exist without infrastructure. And, as is true with almost every disruptive technology, there's a downside — ubiquitous connectivity creates vulnerability to cyber attacks that are designed to siphon cash, access sensitive corporate and individual data, or interrupt operations.

In this whitepaper, Level 3 discusses the impact on cybersecurity that evolving uses of technology have brought about and the strategies that can be employed to help defend against hacking, viruses and worms, botnets and other cyber warfare weapons.

## INTRODUCTION

Today's cybersecurity landscape is rapidly changing. Conventional security standards and practices cannot keep up with the frequency and sophistication of attacks. Between May and July 2011, the industry and governments experienced a sharp increase in cyber attacks against a number of large, technically savvy organizations:

- Sony revealed several major customer data thefts occurred, which affected more than 100 million user accounts (77 million PlayStation Network users and 24.6 million PC games customers).[1]
- RSA, a company that makes one of the industry's most widely-distributed form of two-factor authentication, SecurID tokens, suffered an attack that resulted in RSA replacing 40 million of its tokens.[2]
- In an attack directly related to the RSA breach, defense contractors Lockheed Martin and L-3 Communications were hit by sophisticated attackers who used counterfeit RSA tokens to impersonate the access codes of targeted employees.[3]
- The International Monetary Fund suffered cyber attacks in June, but it did not disclose the nature of attacks or whether a security breach actually happened.[4]
- Citibank reported that credentials for 200,000 users were stolen, including names, account numbers and email addresses.[5]
- Infragard, an FBI-led partner organization, was compromised by hackers in Connecticut and Atlanta, revealing passwords of hundreds of industry and law enforcement users.[6]

*E-commerce, social media companies and revenue streams based on flowing media to audiences around the globe simply wouldn't exist without infrastructure.*

- The identities of border patrol agents in Arizona were released in protest of Arizona's immigration enforcement policies by hacktivists (defined as those who use computers and networks as a means of protesting political ends).[7]
- Websites operated by organizations such as the CIA, the U.S. Senate, PBS and Citibank have been defaced in high-profile attacks by a hacking group called "LulzSec" (hacking for laughs).[8]
- STUXNET, one of the most sophisticated computer viruses on record, specifically targeted and severely damaged an Iranian nuclear facility and signaled the future of cyberwar attacks on critical infrastructure.[9]

These are just a small sample of the daily attacks launched by governments, hacktivists, pro and recreational hackers and criminals. While technical innovation can provide better solutions for cybersecurity, such as more computing power for packet inspection within firewalls, it also can create new areas where attacks can be made. Some of the new technologies that pose an increasing challenge for cybersecurity efforts include:

- **Cloud Computing:** In place of using dedicated hardware servers to provide web sites and other processing functions, enterprises are increasingly using cloud computing resources. The key benefit of a cloud is virtualization. Hardware resources are dynamically allocated to software processes as needed, as opposed to a fixed configuration of software on each hardware server. Attackers see cloud computing companies as prime targets to gain access to multiple companies at once.
- **Mobile Devices:** Many people today carry mobile telephones and tablet computers that have more processing power than previous desktop computers. Coupled with their always-connected state, these devices are literally millions of potential sources of new threat sources and targets for attack.
- **DDoS Attacks:** While there is nothing new about DDoS attacks, some technical evolution is under way. The availability of botnets for hire is increasing the severity of DDoS attacks. Botnets simultaneously bring millions of traffic sources online with the intent of overwhelming websites. They can be controlled using encrypted proprietary communications channels to precisely orchestrate their behavior. As botnets become more sophisticated, they become harder to defeat and more dangerous to victims.
- **Technical Tradeoffs:** As users migrate to high-speed network connections and faster processors, they also expect quicker Internet response times. Technologies, such as deep packet inspection, can parse individual packets looking for virus and other malware signatures. In spite of the increasing levels of processor performance, tradeoffs must still be chosen between network speed and cybersecurity.

[1] http://online.wsj.com/article/SB10001424052748704436004576299491191920416.html

[2] http://www.businessweek.com/news/2011-06-07/emc-unit-rsa-to-replace-security-tokens-after-data-breach.html

[3] http://www.wired.com/threatlevel/2011/05/l-3/

[4] http://gcn.com/articles/2011/06/14/imf-hacked-foreign-government-suspected.aspx

[5] http://www.theregister.co.uk/2011/06/09/citibank_hack_attack/

[6] http://www.huffingtonpost.com/2011/06/21/lulzsec-hack-fbi-partner-infragard-ct_n_881038.html

[7] http://www.azcentral.com/news/articles/2011/06/23/20110623lulzsec-hacks-into-arizona-dps-system-abrk23-ON.html

[8] http://www.huffingtonpost.com/2011/06/20/lulzsec-anonymous-war-_n_880637.html

[9] http://en.wikipedia.org/wiki/Stuxnet

## Counter-attack Strategies

Taking advantage of technologies that help businesses squeeze more productivity from their resources, establish and tap revenue streams, win customers in global markets and (arguably) improve quality-of-life calls for developing and implementing both responsive and proactive cybersecurity strategies. Each player in the overall strategy has a role. Given today's network designs, traffic flow rates, regulatory environment and technical resources, the practical way to increase cybersecurity is a cooperative effort at all levels of the Internet, among users (individual and enterprise), broadband access providers, carriers and government agencies.

*...the practical way to increase cybersecurity is a cooperative effort at all levels of the Internet, among users (individual and enterprise), broadband access providers, carriers and government agencies.*

### Users

End users make up the largest group of Internet participants. Individual users and sophisticated enterprise users connect to the Internet through networks supplied by carriers and access providers.

The best security practice is for users to ensure their devices and networks are free of viruses and botnets. In most cases, these tasks are best performed automatically with virus protection programs and software update utilities.

### Broadband Access Providers

Backbone network carriers are challenged to prevent the propagation of malicious traffic from broadband access providers due to several factors: identifying the source of malicious traffic; the volume of traffic that must be monitored; and their caution in terminating a connection that may carry both legitimate and illegitimate traffic. Traffic from malicious sources is better filtered if those sources are confined to individual network connections. A potential solution for controlling malicious traffic from unsuspecting users is called the "clean pipe" method, enforced by broadband providers. It requires users to have working anti-virus software on their PCs and up-to-date patches, which will prevent general access to the Internet until the machine is properly protected.

### Equipment and Software Providers

Unfortunately, some hardware and software contains defects, which makes systems vulnerable to attacks. Many of these are zero-day defects, while others are introduced by faulty patches or software upgrades applied to existing code that attempt to alter the structure of that code.

Improvements clearly need to be made in commercial software development, testing and release. Already, carriers and other system users are strongly encouraging technology suppliers to improve software development methods, yet software products continue to yield a significant number of security flaws that pose security threats to infrastructure.

### Carriers

Carriers play a key role in cybersecurity, but should not be the sole focus of security initiatives. Carriers can improve network security for users by providing safe, secure mechanisms for domain name system (DNS) lookups. Any incorrect or malicious DNS database entries can severely affect web sites. If a malicious DNS entry redirected a banking website's users to another site, similar in appearance, the malicious website operators could capture users' data, such as user names and passwords, for their own use. Carriers also have the responsibility to provide physical security for equipment installations and other facilities.

*Government agencies at the federal, state and local level have significant interest and responsibility for cybersecurity.*

### Government

Government agencies at the federal, state and local level have significant interest and responsibility for cybersecurity. The federal government can contribute to increased cybersecurity by improving information flow about threats and vulnerabilities among carriers and other parties. New legislation should require significantly improved two-way information flow between carriers and the government about actual and suspected threats must improve.

### Critical Infrastructure Providers

A variety of private enterprises provide infrastructure items that are critical to modern society, including communications, energy, healthcare, finance, food and water. Virtually all of these providers depend on modern communications for routine daily operations and data transfers. Beyond the networks used by telecommunications carriers, autonomous control networks are common within large infrastructure enterprises. Automated systems are used to regulate the supply of electricity within the power distribution grid, convey financial transactions between banks, and control devices used to deliver healthcare and produce food. Ensuring a high level of cybersecurity for critical infrastructure network providers should be a priority for all levels of government as well as the providers. Engaging a network provider that can commit to high levels of reliability and offer a set of security services that help maintain maximum uptime is essential for this group.

## FUTURE DIRECTIONS IN CYBERSECURITY

Beyond the current legislative and regulatory initiatives, significant developments will shape the landscape of cybersecurity for years to come. The following four paragraphs address several of these developments and potential impacts on government networks as well as the public Internet.

### IPv6 Migration

Several issues must be addressed revelant to the federal IPv6 impementation. First, any vulnerabilities arising from publishing addresses inside the DNS network will need to be corrected. Second, when more devices are issued with native IPv6 addresses and connected directly to the Internet (bypassing the Network Address Translation servers commonly used to protect IPv4 systems today), new mechanisms will need to be developed to ensure device cybersecurity. And third, the added complexity required to simultaneously handle two protocol stacks (IPv4 and IPv6) within web servers and other devices will require extra vigilance in design and increased testing to prevent new vulnerabilities.

### Identity Management

Secure, flexible identity management can be easily deployed across multiple platforms with support from carriers. By placing credential servers with the network core, personnel can be verified across multiple agencies' networks. This portability provides greater mobility for staff and improves agencies' abilities to redistribute staff during network outages and public emergencies. Additionally, centralizing these functions could reduce overheads and lower costs.

### FISMA Revisions

Future revisions to FISMA should focus on protecting systems against current and emerging attack vectors. This will help ensure response plans are developed to protect against specific threats. Once agencies start to implement incident response capabilities, those judged to be superior can be shared. Through information sharing and continuous improvement, the overall level of cybersecurity will increase for all federal agencies.

### Future Rulemaking

More complex viruses, worms and other malware are continuously developed at rapid speeds. To keep pace, advanced innovation is needed throughout the cybersecurity industry. Rules and regulations must be flexible to avoid interfering with the development of effective countermeasures. Level 3 agrees with DHS Secretary Janet Napolitano, who said, "We believe that any government rules for cyberspace should identify where we want to be, not proscribe exactly how to get there, and should allow ample space for innovation. They should also be clear, fair and broadly supported, and respect and reflect the diversity of the society in which we live."

*The cybersecurity industry must begin working together as a unified force to prevent these attacks.*

## CONCLUSION

Cybersecurity cannot be achieved through simplistic, rigid rules. Effective defense against cyber attacks requires flexibility to adapt to an evolving array of threats. Cybersecurity adversaries utilize multifaceted approaches to compromise critical infrastructures.

The cybersecurity industry must begin working together as a unified force to prevent these attacks. Each set of users needs not only to protect itself, it also needs to engage in collective, dynamic counter-attack strategies and further adapt regulations that support continued evolution of Internet-dependent technologies.