Cyber-Threat Proliferation

Today’s Truly Pervasive Global Epidemic

During the past year, people around the globe have been captivated—and in some cases, paralyzed—by concerns regarding the spread of the H1N1 flu virus (also known as the swine flu). The powerful strain proves that infectious disease can circumvent the many types of borders we’ve established in architcting our respective societies. Simultaneously, despite the fact that the virus has affected millions of people, sometimes lethally, it’s fair to say that its pervasiveness and implications pale in size and impact when compared to the current global cyber-threat epidemic.

Although it’s perhaps insensitive to juxtapose the implications of a human virus currently wreaking havoc with a set of electronic behaviors that don’t send anyone to the hospital, the current and future risks that cyberattacks pose to our global culture and shared economic systems actually demand the type of attention and concern that H1N1 (thankfully) appears not to have merited. The General Accounting Office of the US government noted a 200 percent increase in cyber intrusions into US government systems in 2009. The concerted situational awareness exhibited by the World Health Organization must be replicated in cyberspace.

Web 2.0

Just as H1N1 is merely representative of the archetype of human virus that medical researchers fear will someday proliferate, prominent cyberattacks such as Conficker represent a pandemic that’s already being played out as cyber criminals use a seemingly endless array of techniques to compromise and infiltrate nearly every aspect of our electronic environment.

Perhaps the best example of today’s global cybersecurity cataclysm can be found in the world of Web applications. Sophisticated criminal networks dispersed across every corner of the planet have undermined the ability of governments, businesses, and common citizens to tap into the incredible utility of the Internet without exposing themselves to the constant threat of information theft or service interruption at the hands of hackers and malware attacks.

As our lives, and for that matter, the entire global economy, have become increasingly dependent on Web-based systems and interconnectivity to operate smoothly, cyberattacks have emerged to stalk us nearly every step of the way; in fact, they’ve grown so complex and varied that traditional IT system defenses such as antivirus (AV) software and intrusion prevention systems (IPSs) have been rendered almost completely obsolete.

Consumer-oriented threats seek to victimize the millions of people who use popular social networking services such as Facebook and Twitter by taking advantage of the trust relationships formed on such sites to steal personal data and infect massive swaths of end-point machines with botnet programs. As well, attackers are increasingly availing themselves of Web-based connections maintained by the IT systems used to manage our world-wide grid infrastructures to manipulate those critical infrastructures or shut them down altogether.

The scope of online threats is only becoming more ubiquitous. During the past year alone, we’ve been confronted with high-profile evidence that these threats aren’t simply anecdotes of what might or could happen, but instead are realities of the current electronic ecosystem. From the widespread compromise of more than 2,500 companies systems by the “Kneber Botnet” to the covert infiltration of Google’s user base (www.bloomberg.com/apps/news?pid=20601087&sid=aUzqFL2tHqqY&pos=9), proof of the dire actuality of the global threat landscape is playing out in our headlines on an increasingly regular basis. Yet these Web-based threats represent a mere microcosm of the attacks being trained on nearly every aspect of information technology. For years before the Internet ever empowered cyber criminals, we experienced attacks directly targeting our network, desktop, and electronic messaging systems that carried the same threat of pervasive infiltration and compromise.
That’s why as we labor to figure out the most effective means by which to go back and harden existing systems and applications and our use of them to account for the cybercrime epidemic, it’s even more important for us to turn an eye toward emerging technologies. As we continue to develop and adopt these powerful mechanisms—including wireless devices, cloud computing, and virtualization—we must remain educated about the risks they’ll incur and stay committed to finding new methods by which to better protect them.

The Future of Electronic Disease

The array of threats we’ll face in the coming years and the range of technologies at which they’ll be directed are only limited by the parameters of engineering and innovation at our disposal. However, threats will primarily be driven, much as today’s attacks, by the rate of adoption of the particular systems and applications we continue to most widely embrace.

As evidenced by the high-profile conviction of hacker Albert Gonzalez on 20 federal felonies tied to cyberattacks he carried out against companies including Heartland Data Systems—a sizable credit-card processing firm that had tens of millions of its customers’ records breached (http://online.wsj.com/article/SB125053669921337753.html)—today’s elite hacker uses multistage attacks that blend techniques and vectors to maintain a persistent and clandestine presence within IT environments.

Subsequently, enterprise security efforts must evolve beyond a focus on resiliency and shift to defense in depth—organizations must appreciate that our adversaries’ goal is to create a beachhead within our networks and applications to try to leverage social engineering tactics to attain their objectives. The most significant threats, both in terms of volume and their potential for success, will most likely materialize in the form of newly conceived attacks trained on users’ end-point devices and on Web 2.0 applications driven by user-provided content. However, the proliferation of mobile devices with powerful computing resources, the adoption of Web-based software-as-a-service (SaaS) tools and cloud computing, as well as the growing use of other applications with distributed architectures that incorporate Web services from multiple application service providers will almost certainly become game-changing drivers of threat activity over the next five years.

At the network level, the migration to IPv6 technologies and the convergence of data and telephony networks with voice over IP (VoIP) and other related protocols will present the opportunity for even more serious threats as assailants take advantage of ever-expanding levels of interconnectivity and applications integration to carry out even broader and more damaging assaults on their targets. Further down the road, the current application security epidemic will evolve into another persistent layer of risk as many of the most widespread and sophisticated attacks are aimed deeper into the IT stack into the domain of embedded operating systems and virtualization technologies.

To tap into the power of Web-based, wireless, and other emerging technologies, and thus build stouter virtual castles in the sky, we must appreciate the evolution of blended threats from the simple virus of yesteryear to the virulent MALFI (multifaceted malware with remote file inclusion, local file inclusion, cross-server attack, and remote code execution) botnet attacks of 2009. Rather than endorsing security models that drive us to construct additional defenses and filters that have an increasingly slim chance of stopping advanced threats, the focus within IT development and security must shift to emphasize more aggressive, proactive self-assessment through which “offense can inform defense.”
Sensitive information being generated, set in transit, and left at rest in cloud computing services all constitute major challenges in being able to prove that those controls actually function effectively.

The Internet, has become one of the fastest growing areas of IT innovation as organizations seek to further avail themselves of the flexibility and economies of scale that Web-based technologies provide.

Lately, people have been scrutinizing cloud computing as it relates to security, now that it’s clear that this major shift in computing infrastructure utilization won’t be realized without the emergence of parallel attacks and related risks. But many cloud computing advocates argue that a more distributed infrastructure will be inherently safer than today’s model, through which organizations maintain and protect most of their own electronic data, because those responsible for building and defending the clouds will have greater incentive to secure them to further their business models.

However, from the IT security side, the practical realities involved in offloading such a wide range of critical computing processes and virtual mountains of electronic data onto third-party service providers or even into self-managed, privately operated clouds represent a daunting new wave of risk. Will a service provider, or even an enterprise maintaining its own cloud, truly be more concerned with protecting its customers’ data, or even its own, than those organizations traditionally have been? The answer is unclear. Anyone familiar with IT security can also recognize that distributed, interconnected clouds create as many potential risks as they eliminate. Here are some reasons to fear for IT security as it relates to cloud computing:

- There is already overreliance on encryption. Encryption is a powerful tool, but if history has taught us anything, it’s that encryption can be defeated, both by technical innovation and human error.
- Virtualization remains an unknown. So much of the cloud computing model depends on the use of virtualization, but researchers, including those at my company’s CoreLabs group, have proven that it’s an unproven commodity with regard to security and that there are significant vulnerabilities in the systems that attackers frequently use.
- Outsourcing is a huge security risk. Organizations handing over their intellectual property and customer data to third parties often pay for it in spades. We’ve seen this risk repeatedly reinforced in the government space related to breaches on the part of contractors and other third parties. Organizations don’t typically make security a major element of their business contracts nor do they write safeguards into their outsourcing agreements. Until they do so and invoke major penalties for subsequent breaches, a pass-the-buck approach to security will continue to dominate.
- The security perimeter will become even fuzzier. Organizations are already struggling with the IT security perimeter softening, especially those parts related to remote access and electronic data sharing. With data constantly available in the cloud for user access in multi-tenant environments, the opportunity for infiltration will grow exponentially.
- Lastly, SaaS applications could leak data even when encrypted: their use of networks can cause side-channel leaks that could enable attackers to glean even the most sensitive of data.

Sensitive information being generated, set in transit, and left at rest in cloud computing services all constitute major challenges, not just in how to enforce security and privacy policies, but also in being able to prove that those controls actually function effectively. Multitenancy and resource usage optimization, driven by economies of scale, are fundamental to the cloud computing model, but they introduce a multitude of security issues due to the blurring lines of demarcation for data that enters and traverses the cloud.

I could point to similar issues in other rapidly maturing areas of IT, such as the proliferation of wireless devices and applications, but the risks tied to cloud computing provide a truly telling example of the newly emerging and complex security challenges that we continue to create for ourselves.

The time to realign our perspective must be now if we’re to prevent the current cyber threat epidemic from becoming further entrenched as an acceptable element of our organizational and personal posture. Much as we have shifted our approach to medical advice and treatment from an almost entirely reactive model to that of preventative medicine throughout the past 100 or so years, we must now rapidly transition our approach to IT security to one of proactive self-assessment that lets us identify and remediate

---

**Head in the Clouds**

Cloud computing, a generic term for any IT system that involves the delivery of hosted services via the Internet, has become one of the fastest growing areas of IT innovation as organizations seek to further avail themselves of the flexibility and economies of scale that Web-based technologies provide.

Lately, people have been scrutinizing cloud computing as it relates to security, now that it’s clear that this major shift in computing infrastructure utilization won’t be realized without the emergence of parallel attacks and related risks. But many cloud computing advocates argue that a more distributed infrastructure will be inherently safer than today’s model, through which organizations maintain and protect most of their own electronic data, because those responsible for building and defending the clouds will have greater incentive to secure them to further their business models.

However, from the IT security side, the practical realities involved in offloading such a wide range of critical computing processes and virtual mountains of electronic data onto third-party service providers or even into self-managed, privately operated clouds represent a daunting new wave of risk. Will a service provider, or even an enterprise maintaining its own cloud, truly be more concerned with protecting its customers’ data, or even its own, than those organizations traditionally have been? The answer is unclear. Anyone familiar with IT security can also recognize that distributed, interconnected clouds create as many potential risks as they eliminate. Here are some reasons to fear for IT security as it relates to cloud computing:

- There is already overreliance on encryption. Encryption is a powerful tool, but if history has taught us anything, it’s that encryption can be defeated, both by technical innovation and human error.
- Virtualization remains an unknown. So much of the cloud computing model depends on the use of virtualization, but researchers, including those at my company’s CoreLabs group, have proven that it’s an unproven commodity with regard to security and that there are significant vulnerabilities in the systems that attackers frequently use.
- Outsourcing is a huge security risk. Organizations handing over their intellectual property and customer data to third parties often pay for it in spades. We’ve seen this risk repeatedly reinforced in the government space related to breaches on the part of contractors and other third parties. Organizations don’t typically make security a major element of their business contracts nor do they write safeguards into their outsourcing agreements. Until they do so and invoke major penalties for subsequent breaches, a pass-the-buck approach to security will continue to dominate.
- The security perimeter will become even fuzzier. Organizations are already struggling with the IT security perimeter softening, especially those parts related to remote access and electronic data sharing. With data constantly available in the cloud for user access in multi-tenant environments, the opportunity for infiltration will grow exponentially.
- Lastly, SaaS applications could leak data even when encrypted: their use of networks can cause side-channel leaks that could enable attackers to glean even the most sensitive of data.
our greatest points of critical risk before attackers assail them.

Government and private sectors must create incentives and penalties that push organizations to put themselves through the necessary forms of examination, the virtual MRI of vulnerability assessment and penetration testing, that will let them minimize these daunting electronic risks that ultimately affect us all. Just as we can’t prevent the most persistent forms of infectious disease, such as the H1N1 flu virus, from circling the globe and infiltrating our lives, we’ll never fully eliminate the opportunity for IT-driven attacks. However, through more intelligent security strategy and process, we can begin to diminish the current state of ubiquitous contagion. The cyber threat has proliferated dramatically in 2010. Cyber-situational awareness is fundamental in combating the elite and highly organized adversities on the Internet.

Tom Kellermann is the vice president of Security Awareness and Strategic Partnerships at CoreSecurity, a professor at American University’s School of International Service, and serves on the Commission on Cyber Security for the 44th Presidency. He is a coauthor of E-Safety and Soundness: Securing Finance in a New Age. Kellermann has a BA from the University of Michigan and a masters from American University’s School of International Service. Contact him at tom.kellermann@coresecurity.com.