

# FIVE NETWORK SECURITY THREATS AND HOW TO PROTECT YOUR BUSINESS

A layered approach to security may be your best defense

## EXECUTIVE OVERVIEW — CONTROL LAYERS TO DO MORE WITH LESS

Threats abound in today's corporate networks. There's no getting around it. Keeping your enterprise and its data and corporate assets secure necessitates a proactive security posture. Being proactive involves understanding the assets that require risk mitigation and the proper controls to support your risk management strategy. This paper uncovers the five most costly network security threats that enterprises battle today and how you can protect your business by implementing key layers of control and taking advantage of managed security services to do more with less.

Security budgets are continuing to feel the strain of the current economy. Unfortunately, network and system threats won't take a break, even in a down market.

## ECONOMIC GAIN FROM THREATS — BUSINESS THREAT IS GROWING

The increasing virulence of attacks over the past 20 years is considerable. Along with the global, connective nature of the Internet, threats have evolved from one-off incidents caused by fame-seeking hackers to organized attacks by malicious parties seeing profit. And as the reliance on IT infrastructure grows, the attack surface increases; there are more opportunities than ever. The trend is evident in the rise of "botconomics" — the joining of botnets to compromise a network in an effort to make money. Compromised digital assets have been monetized and, without proper security controls, are up for grabs.

The economic force driving the underground value chain for stolen data is immense and has evolved to comprise black markets for selling stolen data, mules to carry out purchase transactions using the stolen data, auction market places to resell the goods, and currency transaction services to transfer the ill-gotten funds. Network attacks against major online brands such as Yahoo®, Google™ and Twitter™ have brought the issue to the media mainstream.

Business communications and employee work behavior have evolved to increase the flexibility of where we work, how we access data, and applications we use to communicate. This flexibility has brought about consequences as it introduces new attack vectors to a company's environment. More employees are using devices other than their work PCs to access data and are adopting communication applications that foster collaboration and social networks (i.e. wikis, IM, Blogs, Facebook®, Twitter).

Without the confinement of applications, systems and communications within the corporate network of yesterday, the environment is now more mobile and diverse, and this has a huge impact on how we interact with data. Our workforces on the road or at home can access information from devices other than their PCs. Communication has expanded beyond email and instant messaging to other forms such as micro blogging, now used in the corporate environment. The question is, given this environment, how can you control the spread, or leakage, of data?

Although companies must operate according to certain governmental or industry requirements, and demonstrate to auditors that they are in compliance with those requirements on an ongoing basis, there's always human error. People can unintentionally leak data through email or web sites. Technologies such as link prevention can help to control security mishaps, but they're not fool proof.

Fortunately, you can take steps to prevent threats, but you must first understand where the threats lie. The cost of security is high, including expenses for systems and tools, people and resources to configure and monitor security systems, and the time and material to develop the appropriate processes to ensure everyone adheres to policies. Before allocating your security budget, make sure you're putting your dollars where they will be most effective. A solid understanding of the most damaging threats will help you make informed decisions about your security infrastructure.

## THE FIVE MOST COSTLY NETWORK SECURITY THREATS

Network threats are numerous, but some are more deadly than others. Here are five of the most costly threats:

- 1. Botnets.** In the past, "botnets" were created for fun, and to satisfy the curiosity and egos of rogue hackers. These individuals would manually compromise systems and move on, without leaving too much damage. Today, botnets are virtual chop shops—sophisticated and monetized, they can be used for serious cybercrime. In fact, botnets are the primary vehicle for cyber criminals. They can be used to steal identities from hundreds of people on the other side of the world with a single attack.  
  
Today's botnets are also more resilient. They're built on tiered infrastructure and the technology they use has evolved to HTTP and peer-to-peer channels with encryption. Consequently, they're hard to take down. They can also be managed remotely, so there's a slim chance of finding the culprit.  
  
To combat the botnet threat, companies need security expertise. It's worth the money, because the impact of a sophisticated botnet attack to an organization can be huge, resulting in a tarnished reputation, hefty fines and even lawsuits. And not only large companies need to worry; smaller companies are also at risk.
- 2. Phishing.** The practice of "phishing," or masquerading as a trustworthy entity to get credentials from someone over the Internet, is becoming more and more sophisticated and easy to do. There is a rise of kits on the open market that cost as little as \$49. They enable anyone to copy legitimate sites and set them up for malicious purposes. Phishing is second only to spam for compromising systems on the Internet today, and many are hosted on botnets. Through phishing sites, hackers can harvest credentials of individuals and index them based on many dimensions. The impact is costly, resulting in fraud, stolen identities and compromised data.
- 3. Malware.** There's been an explosion of malware in the last few years. According to a study from the University of Michigan & Arbor Networks Inc. called the Internet Malware Classification and Analysis (2007), 75,000 to 250,000 new families or variants of malware were released in 2006, and that number ballooned to 60,000 to 80,000 per month in 2008. It's estimated that there's a new variant released every 30 seconds. Although antivirus software coupled with intrusion detection solutions is the front line of defense, it fails to detect malware 20–62% of the time.
- 4. Distributed denial of service attacks.** Distributed denial of service (DDoS) attacks are growing in number and in size. DDoS attack size continues to outpace the size of average dedicated Internet access circuits. According to a 2008 worldwide infrastructure security report by Arbor Networks, 57% of ISPs have reported attacks larger than 1 Gbps. Attacks of this size can cause prolonged outages of prominent Internet facing services, such as online bill pay and VoIP.
- 5. Attack sophistication.** Because many companies have put in infrastructure to mitigate simple attacks, the attacks are evolving and becoming more sophisticated, and they're overwhelming network transactions on the back end instead of on the Internet facing side. DNS-based abuses like PRNG name generation, DDoS vectors and rouge DNS servers are common. Another attack vector is the router. Wormable attacks like Conficker can compromise as many as 2 million systems or more. Attacks of this magnitude are difficult for companies to prevent on their own with internal resources, and many are turning to cloud providers who can dedicate the resources to a more sophisticated security system.

## MITIGATING THREATS: THE KEY LAYERS OF CONTROL TO BE MORE PRODUCTIVE

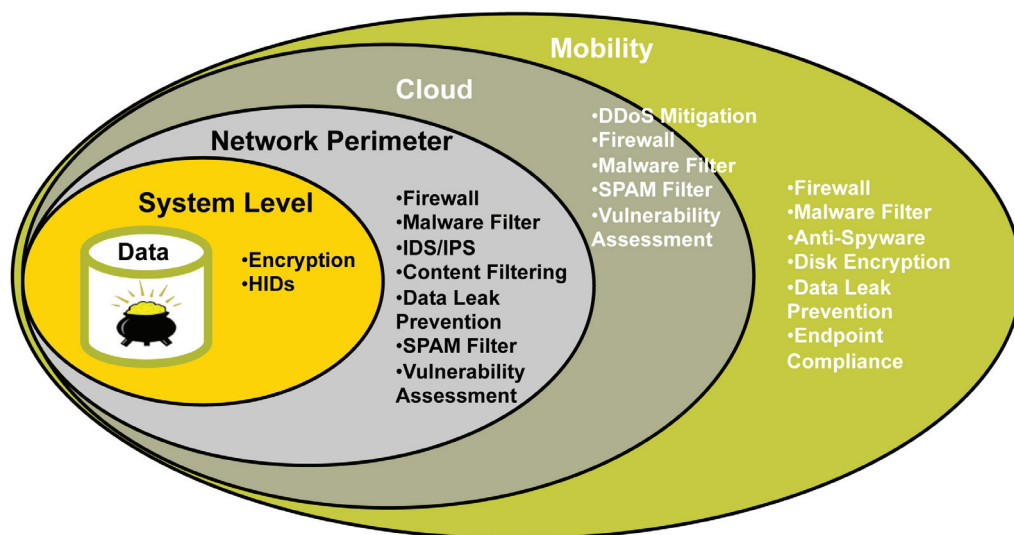
There are some key layers of protection that should be implemented to provide effective threat prevention and mitigation. For example, service providers can deliver security services to prevent the effects of phishing on enterprises by screening traffic before it enters the enterprise network. This capability enables users to be more productive, as well, because it lowers the infection risk and rate, and removes the burden of deleting spam and filtering out bad email.

To fight malware, organizations need a combination of anomaly detection, customer premise equipment and ISP in-cloud security systems. When implemented only at the network's perimeter, Intrusion Detection or Prevention Service (IDS/IPS) devices will drop unauthorized packets but cannot prevent a DDoS attack, because the number of packets would cause disruption to the Internet link. If you mitigate DDoS attacks in the cloud, the packets are dropped in the cloud, so only filtered traffic would travel to the corporate network. Using cloud services mitigates security issues away from the network to preserve people and resources, is often transparent to users and requires no additional hardware or software to be installed on the premise.

Another security challenge involves the increasingly mobile workforce. Most companies have security at the perimeter because, historically, most system attacks occur there. However, as more employees work remotely, there's a need to expand security to the laptop and other mobile devices and enforce endpoint compliance. One interesting technology available is endpoint compliance software offered by companies like Symantec, Checkpoint and Fiberlink. This technology allows you to enforce that end users use firewall and antivirus software any time they access the network remotely. Endpoint compliance software enables you to ensure all endpoints are compliance with corporate security policies by pushing out the latest patches and updates. In this way, you can be certain remote access points are not vulnerable to the latest exploits.

There are a multitude of technologies available for each layer of the network. It's important to layer on all of these technologies for complete protection against all possible threats:

- System level: Encryption and Human Interface Devices (HIDs).
- Network perimeter: Firewalls, malware filters, IDS/IPS systems, content filtering, data leak prevention, spam filters and vulnerability assessments.
- Cloud: DDoS mitigation, firewalls, malware filter, spam filters and vulnerability assessments.
- Mobile devices: Firewalls, malware filter, anti-spyware, disk encryption, data leak prevention, and endpoint compliance.



## DO MORE WITH LESS — WORK WITH A PROVIDER TO INCREASE SUCCESS

Security budgets are continuing to feel the strain of the current economy. Unfortunately, network and system threats won't take a break, even in a down market. The financial consequences of a breach will be even more devastating, so it's important to invest wisely when planning your network security strategy.

Evaluate the attack service in your network and determine what areas are critical to your business. As you anticipate your company's future security needs, you may decide to partner with a service provider who can offer expertise and resources that you don't have in-house. The benefits include predictable costs and solutions that have been designed, implemented and vetted in production environments. Working with a provider, you can avoid technology obsolescence and offload the heavy lifting while redirecting your own resources to revenue-generating efforts.

Whether you take on the task of securing your network alone, or consult a partner, don't ignore the threat, and take a layered approach to protect your network from every angle.

## CONNECT. SIMPLIFY. ENHANCE.®

with Qwest Business Solutions®



Qwest is focused on helping you work smarter, with services that leverage the latest technology and award-winning support. Here are a few solutions that can address the issues covered in this solutions brief:

### MANAGED SECURITY SERVICES

With Managed Security Services, Qwest can administer and monitor your network on your behalf while you concentrate on other mission-critical elements of your business. Let Qwest allow you to focus on what's important—your business. And, save you time and money through the use of our expert tools, skills, and processes to improve system uptime and performance, optimize security investments, improve employee productivity, and demonstrate compliance. Tools such as Qwest Anti-Virus/ Anti-Spam, Qwest Web Defense, and Qwest Managed Firewall create layers of protection to help reduce the costs and complexity associated with managing security while preventing the impact of security threats.

### WHY QWEST

Qwest delivers reliable, scalable data and voice networking solutions, across one of the U.S. largest fiber footprints. Qwest serves businesses of all sizes, ranging from small business to 95 percent of Fortune 500 companies, with industry-leading SLAs and world-class customer service.

### LEARN MORE

For more information about Qwest voice and data services for large businesses, visit [www.qwest.com/business](http://www.qwest.com/business) or call (877) 816-8553 to speak to a Qwest representative.