


DDoS Threatens Financial Institutions – Get Prepared!



"IF YOU ARE CONNECTED TO THE INTERNET OR HAVE A NETWORKED ENVIRONMENT, YOU ARE AT RISK. KNOWLEDGE OF AND PROACTIVE ACTIONS TOWARDS TECHNOLOGICAL, CYBER, AND OPERATIONAL RISKS THAT THREATEN YOUR NETWORK IS IMPERATIVE!"

**Prepared By:
Susan Orr
Senior Technology Risk Consultant
ReymannGroup, Inc.**

CONTENTS

Could it happen to you?	3
How does a DDoS attack happen?	4
What will you do when it occurs?	4
Is BCP mandated?	5
What are the risks from a DDoS attack?	6
What are the legal and regulatory mandates?	6
How can an ISP help?	7
Are you prepared?	8
• BCP Check-list	
About ReymannGroup, Inc.	8

THIS PAPER PROVIDES AN OVERVIEW OF THE INCREASED THREAT TO YOUR FINANCIAL INSTITUTION FROM DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS AND HOW TO DEFEND YOUR NETWORK FROM SUCH ATTACKS.

COULD IT HAPPEN TO YOU?

It's 7:30 a.m. in the morning and just like every other day you grab a cup of coffee as you head to your office at MyBank to begin your day. As you are settling in the phone rings, you answer it and on the other end is a voice instructing you to wire money to a Western Union account in eastern Europe or the attacks on the network will continue.

What happened to MyBank was not a fluke or unique.¹ Financial institutions' growth in online banking, networking and access to the Internet has led to an alarming increase in operational, reputation, strategic, and systemic risks not to mention real time attacks like distributed denial of service (DDoS). Real time disruptions occur quickly, without warning, and many times with devastating results. The time from release of a newly discovered vulnerability - a weakness that allows specific threats to compromise computer systems - until the actual attack is decreasing from days to seconds. Security experts report it takes as little as six seconds for a launched attack to find and infiltrate an unsuspecting system. The skills needed to launch attacks are also decreasing with sophisticated automated software as displayed in Figure 1.



Figure 1

These automated attacks have changed the attack landscape and the motives for launching them. The primary objective for attacks used to be bragging rights and recognition of hacking skills. Today, the attacks are being launched for financial gain. Organized crime is now enlisting the aid of and incorporating the techniques of hackers for criminal intent such as identity theft, online

¹ Similar large DDoS attacks have been reported in the press for payment gateway companies and financial institutions such as Authorize.net, PSIGateway, Worldpay, 2checkout, Royal Bank of Scotland and others.

fraud, and extortion. Real time cyber crime attacks are now listed as the FBI's third highest priority, behind terrorism and espionage. Financial institutions that are subject to a real time attack could be exposed to significant losses in earnings and capital due to the loss of customers, cost of repair, and damage to reputation. According to Computer Economics, Inc., lost revenue and repair costs from attacks on networked services and disruptions in 2005 are expected to exceed \$17.5 billion, up from 13.2 billion in 2003.

While many institutions have implemented controls to respond appropriately to many of the threats identified in Figure 1, a DDoS attack creates a new and different threat that must be addressed. As an institution continuously monitors and adjusts its technology risk management program, it must identify and respond to emerging threats. DDoS attacks have emerged as a significant threat for business continuity and security of Internet facing services. Distributed denial of service attacks are too easy to execute.

HOW DOES A DDoS ATTACK OCCUR?

There are several types of denial of service attacks but the most common attack involves flooding the links into the data center and any Internet facing servers, which eventually overwhelms the infrastructure until it shuts down. Your data center will be disconnected from the world. No amount of redundancy can prevent this from occurring. Even with two data centers, historical events have shown that this type of attack can flood links to all redundant data centers. The vast majority of today's denial of service attacks are distributed, which entails taking over numerous computers of unsuspecting parties often referred to as "bot" or "zombie" computers.

Hackers that know how to create spam machines or spyware can generate DDoS attacks. In addition, a DDoS attack is generated with the help of many (potentially hundreds of thousands) unsuspecting zombie machines and it is not possible to stop the DDoS or protect your network with traditional security measures. Such attacks make it much easier for the perpetrator to cover his or her tracks since they are using the computers of innocent people.

Commandeering innocent PC's for a bot or zombie army is a task that is too easy. Hackers search the Internet for unprotected computers, ones with an open port, or not protected by firewalls and intrusion detection controls. Chat rooms, instant messaging, and peer-to-peer networks are fertile ground for acquiring bots. When a hacker finds a vulnerable PC, they install a program on the system that runs undetected in the background of the new bot. The bot or zombie computer then serves the wishes of the hacker sending spam messages and launching DDoS attacks, while the PC owner works away unaware. This smoke screen makes it virtually impossible to trace the attack to the hacker.

WHAT WILL YOU DO WHEN IT HAPPENS TO YOU?

No one is safe. If you are connected to the Internet or have a networked environment, you are at risk of a DDoS attack. Financial institutions are at risk as they conduct transactions and share information with customers, business partners, and vendors over networks and the Internet. Collectively, financial institutions are recognized as one of eight critical infrastructures. The economic stability and public trust and confidence in financial institutions is imperative. Therefore, it is crucial that a financial institution's systems and operations are resilient and the effects from unexpected disruptions are minimal.

Many institutions and their service provider partners are spending significant resources and capital to establish a secure network infrastructure with multiple layers of physical, technical and

administrative security controls to ensure business continuity and security. The DDoS risk, however, has emerged as a significant exposure that can circumvent existing business continuity and security programs. An effective business continuity plan (BCP) is essential to ensure the availability of services at all times and disruptions in service are minimized. Therefore, financial institutions must have an effective BCP and it must address the risk of a DDoS attack.

In the case of MyBank, it is clear that real time attacks such as DDoS can have a significant effect. These types of attacks can disable a website or shut down your Internet facing systems causing a disruption or complete unavailability of resources and services.

Knowledge of and proactive actions towards technological, cyber, and operational risks that threaten your network is imperative. In this decade, proactive risk management is a legal and regulatory mandate.¹

IS BUSINESS CONTINUITY PLANNING MANDATED?

In the past, a BCP was no more than a disaster recovery plan, a process that concentrated on simply recovering the systems. In today's environment recovery is important; however, the plan must also include a process to identify foreseeable risks and threats as well as detect and mitigate logical disruptions, like DDoS attacks. This is especially true for regulated businesses like financial institutions. The BCP should be dynamic reflecting the current risk profile and ability to respond to emerging technological and cyber security threats. In addition, the BCP and infrastructure security should be tested periodically to ensure they remain effective over time, and employees should be trained on all procedures and controls. For example, consider benefits of a well-developed and tested BCP in response to the DDoS blackmail attempt at MyBank.

The morning of the extortion call, MyBank began receiving complaints from customers and employees that they could not access the network. In a matter of minutes the complaints began to increase, customers and employees were now being dropped from the network altogether. Soon after the disruptions began the network shut down completely. MyBank was experiencing a DDoS attack, but since its BCP did not address this type of a problem there were no detection, mitigation, or incident response strategies in place. Management was completely unaware of what was actually happening until they received the extortion telephone call.

Conversely, let's look at another Bank (ReadyBank), which also experienced the same type of attack; however, it had prepared a thorough BCP. ReadyBank had developed, tested and implemented procedures for handling DDoS attacks and had an organized incident response plan. ReadyBank was aware of the potential for such attacks and had proactively coordinated with its managed hosting and Internet service providers to implement detection and mitigation strategies. It was able to detect and react to the attack as soon as it began. The strategies that ReadyBank and its service provider implemented included tools to detect anomalies and DDoS attacks. It was able to proactively redirect traffic from Internet facing systems. Customers and employees were notified within minutes of the temporary disruption in networked services and directed to other delivery channels.

Both of these scenarios are based on factual events that could happen to you.

¹ Gramm-Leach Bliley Act of 1999, Sarbanes Oxley Act of 2002, USA Patriot Act, California Senate Bill 1386.

WHAT ARE THE RISKS FROM A DDOS ATTACK?

Distributed denial of service attacks pose many risks to financial institutions, and can result in a significant loss of time, customers, money, and compliance violations. Potential systemic risk will vary from institution to institution and depend upon the disruption and damage associated with the attack. Common risks that institutions face are operational, reputation, legal and regulatory.

- Operational risk may arise from fraud, error, or unavailability of products or services.
- Reputation risk can stem from operational disruptions, which include errors, delays, omissions, unavailability of information or service, or unauthorized access to information.
- The institution may also find itself subject to regulatory and legal risks – lower examination ratings, increased regulatory scrutiny, civil monetary penalties, enforcement actions, and class action lawsuits - if they have not complied with regulatory mandates for establishing an ongoing and effective BCP and technology risk management program.
- In a broader sense, systemic risk could include the failure of one participant in a transfer system or financial market to meet its required obligations causing others to not be able to meet their obligations when due, causing significant liquidity or credit problems or even threaten the stability of financial markets.²

WHAT ARE THE LEGAL AND REGULATORY MANDATES?

Distributed denial of service attacks are easy to execute and create a significant exposure to business continuity. Such attacks cannot be ignored, immediate action is essential to detect and mitigate the effects. Since attacks cannot be prevented, detection is imperative. The best defense is to implement a process of layered security, comprehensive coverage that employs multiple detection methods and has the capability of preventing the execution of attacks. Detecting and mitigating attacks is a regulatory requirement and can be a challenge for financial institutions. Prudent technology risk management, which includes BCP and incident response planning, is not just industry best practices – it is mandated for financial institutions. In fact, the lack of providing appropriate risk management is considered an unsafe and unsound banking practice.⁴

Specifically, the Federal Financial Institution Examination Council (FFIEC) requires all financial institutions to proactively mitigate the risk of service disruptions and establish a BCP with recovery capabilities. In order to limit or mitigate the effects from service disruptions that can be created by a DDoS attack, financial institutions should implement technological and process controls and coordinate with service provider partners (such as managed hosting or Internet service providers) to ensure they have adequate controls in place.

- *Technological controls* typically include firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and encryption.
- *Process controls* typically include the identifying and monitoring of risks, developing a BCP, installing patches, generating and reviewing log files, e.g., network traffic logs, firewall events, remote access.

² The term systemic risk in this context is based on the international definition of systemic risk in payments and settlement systems contained in “A glossary of terms in payment and settlement systems,” Committee on Payment and Settlement Systems, Bank for International Settlements (2001).

⁴ Office of the Comptroller of the Currency, Bulletin 2004-20.

Industry best practices from organizations like SANS, the National Institute of Standards and Technology, the Information Systems Audit and Control Association mirror the technological and process controls established by the FFIEC. There are numerous international and federal regulations governing business continuity and risk management as outlined in Figure 3. The FFIEC agencies have also issued numerous mandates, which require the awareness and identification of vulnerabilities and threats and implementing processes and controls to detect and mitigate attacks.

Laws & Rules	Regulatory Mandate	Best Practice
Gramm-Leach-Bliley Act Data Protection of 1999	<ul style="list-style-type: none"> • Protect security and confidentiality of customer's non-public personal information • Implement administrative, technical, and physical safeguards • Protect against anticipated threats and hazards to information security • Protect against unauthorized access to or use of information • Establish disaster recovery and business continuity program • Establish a comprehensive written information security program 	<ul style="list-style-type: none"> • Identify vulnerabilities and threats • Establish security controls • Monitor environment • Business continuity program • Ongoing vulnerability analysis • Security program • Employee security awareness • Secure network infrastructure • Protect information assets • Rapid incidence response • Strong authentication methods • Risk management and risk mitigation processes • Detection, protection and response processes • Encryption • Incident response and rapid reporting • Security controls • Detection and mitigation strategies • Board oversight • Employee and customer awareness
Sarbanes Oxley Act of 2002	<ul style="list-style-type: none"> • Secure information infrastructure • Implement internal controls • Safeguard information assets • Monitor IT processes 	
USA Patriot Act	<ul style="list-style-type: none"> • Implement risk based systems and monitoring 	
California Senate Bill 1386	<ul style="list-style-type: none"> • Implement monitoring and reporting systems to identify security breaches 	
Basel II	<ul style="list-style-type: none"> • Monitoring of risks • Business continuity plans • Implementation of risk mitigation 	

Figure 3

HOW CAN AN INTERNET SERVICE PROVIDER HELP?

Implementing the mandated risk management, security and business continuity strategies can be difficult and may not be feasible if you do not have the resources or skills in-house. Deploying the technology in-house is costly and difficult to scale to the size of the attack because the attacks can be bigger than the links to the Internet. The best place to mitigate is at the core of the Internet backbone. Therefore, it may be necessary and more economical to outsource this function or coordinate with your existing managed hosting and Internet service providers. For example, leading Internet service providers (ISPs) such as MCI, AT&T, and Sprint have launched managed DDoS mitigation services to stop these types of attacks.

Many institutions find that contracting technology related services enables them to provide enhanced services economically and more effectively.

The reliance on networked systems, increasing real time risks, ease of executing attacks, and increasing regulatory mandates has changed the business landscape. The board of directors and senior management have a fiduciary responsibility to all stakeholders to ensure their infrastructure is protected, information is available when needed, and systems are resilient. Regardless of the size of your organization, you need to ensure compliance with laws and rules and implement proactive risk management incorporating people, processes, and technology throughout your infrastructure and your service providers. In short, you need to maintain a well-defended and compliant network.

ARE YOU PREPARED?

Quickly assess whether you have proactively addressed business continuity, and detection and mitigation of real time attacks. Use the “BCP Self-assessment Checklist” to start a high-level review of your readiness for responding to threats.

BCP Self-assessment Checklist

Do you have:	YES	NO
1. A networked environment?		
2. Mission critical Internet facing servers / services?		
3. A BCP that covers prevention, detection, mitigation, and recovery of critical IT systems?		
4. A BCP that addresses: <ul style="list-style-type: none"> • Identification of foreseeable risks and threats • Threat scenarios i.e. DoS, DDoS, network intrusion • Strategies for maintaining, resuming, and recovering operations in the event of specific attacks • Technological controls • Process controls • Customer notification 		
5. Real time attack detection strategies in place?		
6. Mitigating controls for identified threats?		
7. A dynamic plan?		
8. Regular testing of the plan to ensure effectiveness?		
9. A process for monitoring risks and threats?		
10. A process for monitoring the effectiveness of the controls?		

ABOUT REYMANNGROUP, INC.

ReymannGroup, Inc. provides finance, healthcare, retail and manufacturing subject matter expertise. We assist companies in evaluating their information security infrastructure, determining exposure to vulnerabilities and threats, prioritizing solutions, and complying with legal and regulatory requirements. We provide you with "independent" high-caliber professionals, authors of regulations and books, and subject matter experts familiar with financial, healthcare, retail and manufacturing industry regulations and best practices. Our experts will meet and exceed your business need. For more information contact or e-mail us at (410) 286-9505 or info@reymanngroup.com. Learn more at www.reymanngroup.com.