



**TEAM CYMRU**

[WWW.CYMRU.COM](http://WWW.CYMRU.COM)

“The Risk of Operating in an Inter-Connected Society”

Jerry Dixon

April 2008

## Overview

The Internet has become essential to many organizations in achieving their business objectives, whether private or public. Technology continues to enable many organizations to rapidly share or exchange information to support just in time manufacturing and electronic commerce, manage process control systems, and increase productivity through automation. However, there are considerable threats and risks to adopting and leveraging these technologies in supporting our organizations. This paper will provide an overview of the current environment and steps you can take to minimize your risk in our inter-connected world.

This rapid adoption of information technologies that has allowed many companies to compete on a global scale is commonly referred to as globalization. This has led to an increasing number of companies leveraging cheaper suppliers of goods or services throughout the globe, enhancing market competition. In order to conduct business with these partners, more companies are connecting their networks with their suppliers via the Internet, which is the backbone, to facilitate the use and sharing of data. Companies that normally compete with one another in the global marketplace might often team up to jointly go after a large business opportunity, which will often involve a connection between their networks to facilitate collaboration and project tracking. These are just several examples that show how inter-connected we are and how dependent we are on the Internet. It is a cost-effective medium utilized by many organizations that enables business on a global scale. To show how essential the Internet and networking technologies are to the government, a group called the Network Centric Operations Industry Consortium was created and has the following in their mission statement (2004), "Our mission is to facilitate global realization of the benefit inherent in Network Centric Operations. To that end, we seek to enable continuously increasing levels of interoperability across the spectrum of joint, interagency, intergovernmental, and multinational industrial and commercial operations. We will execute this mission in good faith as a global organization with

membership open to all enterprises in quest of applying the vast potential of network centric technology to the operational challenges faced by our nations and their citizens.” They further add, “From 9/11 to Hurricane Katrina and Operation Iraqi Freedom, access to information, or lack thereof, has been the determinant of life or death.” This demonstrates how critical the Internet is for the sharing of data, and the use of technology to collaborate in the marketplace and in the public defense/safety arena.

### The Sophisticated Threat Landscape

However, there are many threats to consider in our inter-connected world and the days of opportunistic hackers have been replaced with a more organized and sophisticated group of attackers that include organized criminal groups, nation states, companies engaging in competitive intelligence gathering, and non-state actors. They often work to take advantage of vulnerabilities or improperly configured systems that put critical services, data, and critical infrastructure at risk. The sophistication of these attacks continues to be problematic, as new vulnerabilities are discovered at an alarming rate, and popular websites continue to be compromised with embedded malicious software, which can immediately compromise the computer of a user visiting that web page. This type of attack requires very little user interaction besides opening their web browser and going to visit a website they thought was safe. Often the user’s computer, unbeknownst to them, will be redirected to other sites on the Internet that will install additional malicious software to either steal data from them, use it to gain access to their employer’s network, or incorporate their machine into a BOT net for the purposes of attacking other sites through denial of service attacks or stealing information. The very inter-connected nature of our networks presents some unique challenges; where we once had good control over managing our users, often referred to as insiders, we are now in an age of virtual insiders that often change rapidly based on business partnerships.

To highlight how organized the digital black market is we will look at an organization called the Shadowcrew. McCormick and Gage (2005) provide a glimpse into how the mobs of the physical world have moved into the digital realm. They go on to state the following, "They buy and sell millions of credit card numbers, social security numbers, and identification documents, typically less than 10 bucks a piece (p. 1)." They further state that Shadowcrew "consisted of more than 4,000 members worldwide, ran a worldwide marketplace in which 1.5 million credit card numbers, 18 million email accounts, and scores of identification documents-everything from passports to driver's licenses to student identification-were offered to the highest bidder (p. 1)." The United States Secret Service investigated the ShadowCrew, taking more than a year to gather in-depth knowledge of how they were organized and how they operated. The "Shadowcrew consisted of a governing council, enforcers, moderators, reviewers, vendors, and general members" as outlined in McCormick's and Gage's (2005) report on Shadowcrew (p. 5). It is alarming to note that organized crime has finally caught up with the technology age and how quickly they have adapted to the digital world by going after the millions of users that use the Internet for email, on-line shopping, and web browsing. Taking advantage of this marketplace is this reason that organizations such as Shadowcrew have popped up on the Internet. To make it an even more lucrative proposition, they have set up websites to train others in identity theft, credit card theft, and have even created templates for others to build phishing emails. They also provide mechanisms to hide their online identities by using techniques to obfuscate how they are connecting to the Internet, thus making it more difficult for law enforcement to identify who is perpetrating the crimes. The ease of concealing your identity, while all the while stealing the personally identifiable information of others, makes moving to the digital world very attractive to criminals. This concept is highlighted in an interview with Marty Lindner with the Carnegie Mellon University Computer Emergency Computer Coordination Center (2006) who states, "Our societies increasing reliance on electronic information has made it possible for bad actors to gain an advantage by simply using information. In the past, bad actors needed to confront their victims to gain an

advantage. For example, bank robbers using guns to get money from a bank. We don't see much of this anymore. Now they just need to get a username and password to achieve the same goal (p. 1)." The expectation is that more organizations like Shadowcrew will migrate towards the Internet since it has no geographical boundaries and making it difficult to identify and capture on-line criminals.

In the Shadowcrew case, according to McCormick and Gage (2005), "the Secret Service was able identify members due to a well placed informant (p. 3)", much like many of the mafia cases of the past. If it were not for the informant, there would have been many more victims due to Shadowcrew's proficiency in the on-line trade of credit card information and ability to cover their tracks. In this particular case, law enforcement was able to catch them in the act and able to take swift action once key members were identified. They did this through wiretaps and network sniffing devices that were approved by the US Courts to catch Shadowcrew in the act of transmitting stolen credit card information.

#### The target: Your PII

One of the major objectives of online attackers is to gain access to "Personally Identifiable Information" (PII). This is information that is linked to you as an individual, such as your social security number, date of birth, driver's license information, financial information, or medical information. This information is also essential for many organizations to conduct business but as illustrated, there are many challenges in protecting this information. As you might be aware, there has been a noticeable increase in media reporting about loss of this sensitive information and an increase in "New Account Fraud." The numbers of affected individuals are in the millions. Breaches or compromises of this data are often a result of dependence on network inter-connections with third-party credit card processors, business partners, or bad security practices. Some recent examples of compromised PII are described in the following paragraph.

A recent story by Brian Krebs from the Washington Post (2008) states the following, *“The Hannaford Bros. supermarket chain said this week that a breach of its computer systems may have given criminals access to more than 4 million customer credit and debit card numbers.”* The article also goes on to further quote the CEO of Hannaford, *“Hannaford chief executive Ronald C. Hodge said in a statement that the stolen data included credit and debit card numbers and expiration dates that was illegally accessed from the company's computer systems while transactions were being processed and authorized.”* Stories like these are published on a weekly basis, and while serious, are treated as nearly “normal”, where a few years ago this type of breach would be unprecedented. Some of these data breaches are the result of poor configuration management practices, such as this one reported recently in the Baltimore Sun by Liz Kay (2008); *“Maryland dental HMO acknowledged this week that it had accidentally posted the names, addresses, and social security numbers of 75,000 members on its website.”* It is not always the result of an attack, but of organizations not properly protecting our personally identifiable information.

### What can you do?

Now let us discuss what you can do to protect your networks and information, whether you are a government or private sector organization. Whether you're the chief information officer or a member of the information technology staff, you need to make sure you know where the data is stored and where it is being utilized. The first step in this process is to develop a policy for your organization that clearly highlights what personally identifiable information is and how it's handled. To make this a comprehensive policy it should cover all aspects of handling personally identifiable information whether electronic or paper, data retention, usage, and destruction. Also be sure to consider your business partners and contractors, did you include language in the contract to ensure you both will protect the shared personally identifiable information? By the way, those computers you just donated to charity, did you sanitize the hard disks? What about all of those tape backups, flash drives or portable storage

units? How are the tape backups protected? What about when it's in transit to offsite storage? These are just a few things to consider when evaluating how your organization handles personally identifiable information and developing a formal policy and procedures.

There are many technologies available to help us to protect our networks and sensitive information. There are tools from database vendors that allow you to encrypt certain sensitive fields or data mask them. The fields that would commonly need protection are:

1. Social Security Numbers
2. Drivers License Numbers
3. Credit Card Numbers
4. Credit Card Verification Numbers (which should never be stored after transaction processing is complete)
5. Account Numbers
6. Any other information that can be used to identify an individual

By data masking or encrypting only sensitive fields within a record, you can ensure that you get the database performance needed, overcoming one of the reasons many organizations cite for not leveraging database encryption. There are tools to encrypt and protect data on desktops and laptops that allow you to specify a specific directory or an entire hard disk. This will help mitigate the risk of a stolen computer by protecting the contents on the hard drive. As we highlighted, you should protect data where it resides but also protect it while in transit as it traverses networks. There are hardware based encryption accelerator cards available to help with minimizing impacts to performance and in today's technology world performance is not an excuse for not protecting personally identifiable information. Another technology solution that should be evaluated by your organization is products that enforce role based access control coupled with two-factor authentication. This limits how the information is handled and ensures only those with the need to read or manipulate the data have the ability to do so, while preventing access by others whose job role does not require working with PII.

Maybe they only need to read part of the information such as the last four digits of a social security number to confirm who they're talking to on the phone but don't need the full social security number associated with the individual. You can provide granular access controls based on job function. That said, we don't recommend using a social security number as an identifier or for security purposes, as it is a primary route to identity theft. Instead, use some other piece of information that only your organization and the individual you're trying to identify will know, this is called a "shared secret."

Now on to the real issue with handling of personally identifiable information by those that need to utilize that information. It's all about the user and maintainer of the information. Which leads us to how important security awareness programs are within any organization; whether you're in management, a user, or part of the information technology team, everyone has to understand what the policies are, how to handle the information, and where within your organization to report a cyber security incident. This will enable organizations to contain a potential compromise of personally identifiable information quickly by providing a place to report a compromise or suspected compromise of data. It will allow them to minimize the potential number of victims and communicate quickly with those affected. The cyber security awareness program should be a part of the new employee orientation and be conducted quarterly to re-enforce the importance of protecting personally identifiable information, corporate sensitive data, and systems.

Also, don't forget that good life-cycle management is essential to protecting your critical systems and data. To give you an example, while working incidents in the past with very large organizations, they were not able to properly update their routers with the latest security fixes due to the hardware being unable to support the patches. In one case, they had not updated their hardware in over seven years which made them extremely vulnerable to remote based network attacks via the Internet. They had asked who was behind the attacks and upon doing network forensic analysis it was more of a question of who wasn't in their networks. This highlights that you have to have a comprehensive program to properly do life-cycle management of your information

technology infrastructure and patch management. This includes following good change management practices. As illustrated earlier, a change was made to a Dental HMO's website that put over 75,000 of their customers' sensitive information right on the Internet. This could have been averted if they had good change management procedures in place. Another major threat to your data is the introduction of malicious software through email, malicious websites, or via a business partner that you have network connectivity with. In the early days of the Internet, it often required the user to click on an attachment or take some action to install malware on their system. In today's environment, they can simply be compromised by browsing to a website that they thought was safe. Team Cymru, in a thirty day period, saw a new piece of malware coming out every 2.2 seconds and within the first day of it being identified only 38% of anti-virus products detected them. Unfortunately, there are no silver bullets to tackle these challenges but there are many ways to contend with these threats. Many security companies provide a wide range of services such as content filtering for web and email traffic, enterprise anti-virus, patch distribution systems, and of course, host or network based intrusion prevention systems. All of these solutions are needed along with non-signature based protections such as network flow analysis tools to monitor outbound traffic to determine if you've been compromised or have problems on the inside of your network. To make this an even more effective approach your organization should procure cyber-intelligence information so that you at least know what are the top sources of threats, top malware threats, and can look for problems at your network perimeter. The cyber attackers are sophisticated and to level the playing field you should be too. They rapidly share techniques and tactics to gain access to your data therefore you should understand what those are by increasing your situational awareness through cyber intelligence.

In conclusion, in order to properly protect your data and networks in this highly inter-connected world you need to do the following:

1. Determine what data and networks are critical to your business.

2. Develop a risk management based approach to protecting your critical data and networks.
3. Identify where and with whom you're sharing proprietary and consumer information with then apply appropriate risk mitigations.
4. Implement a Security Awareness Program and provide a place for employees to report suspected security problems, such as a corporate incident response team.
5. Have your Information Security Team get connected to cyber-intelligence information so they can stay on top of emerging threats and vulnerabilities.
6. Ensure you have a security architect team involved early on with the potential adoption of new IT projects or technologies.
7. Make sure you have an incident response annex within your business continuity plan to help contain, recover, and take lessons learned to improve current processes and technologies deployed within your organization to mitigate similar incidents in the future and ensure your organization is prepared.
8. When working with third parties or business partners make sure you work with your legal team to have language added to the contracts that protects the data, data in transit, and that the partner takes reasonable measures to protect the information similar to your own. It should also spell out legal relief if they mishandle the information or have a data breach due to not having taken appropriate measures to protect the data or networks.
9. Enforce technology lifecycle refreshment cycles and have a patch or security fix deployment solution in place including good change management procedures.
10. Test your applications, networks, and procedures through penetration testing, vulnerability scanning, and ensure policies are being followed.

## Works Cited

Kay, Liz F. "No sure bets in personal data security, Recent HMO Breach only one among many." Baltimore Sun 28 Mar. 2008:1A, 9A

Krebs, B. (2008). "Grocer Says Data Were Compromised" Retrieved March 28, 2008 from <<http://www.washingtonpost.com/wp-dyn/content/article/2008/03/18/AR2008031802878.html>>

Lindner, Martin. Senior Internet Analyst, Carnegie Mellon University.  
Personal Communication: 2005. 412-268-3107. [mml@cert.org](mailto:mml@cert.org)

McCormick, J., Gage, D. (2005). *ShadowCrew: Web Mobs*  
Retrieved November 20, 2005, from  
<[http://baselinemag.com/print\\_article2/0,2533,a=147349,00.asp](http://baselinemag.com/print_article2/0,2533,a=147349,00.asp)>

Network Centric Operations Industry Consortium. About NCOIC&Mission Statement. 24 Aug. 2004.  
<<https://www.ncoic.org/about>>  
<[https://www.ncoic.org/about/mission\\_vision/](https://www.ncoic.org/about/mission_vision/)>