Sponsored by

CIPHEROPTICS
Simply Secure

Ponemon Institute LLC

Network Security 2.0

Presented by Dr. Larry Ponemon
August 13, 2007

Network Security 2.0

Presented by Dr. Larry Ponemon, August 13, 2007

1. About the author

Dr. Larry Ponemon is the chairman and founder of Ponemon Institute, a “think tank” dedicated to advancing responsible information and privacy management practices in business and government. The Institute conducts independent research, educates leaders from the private and public sectors, and verifies the privacy and data protection practices of organizations.

Dr. Ponemon is considered a leading international expert on privacy auditing and responsible information management. He has extensive experience in auditing self-regulatory frameworks for data protection and privacy compliance in the United States, Canada, the European Union, Hong Kong and other nations.

Dr. Ponemon was recently appointed by the White House to the Data Privacy & Integrity Advisory Committee of the Department of Homeland Security. Previously, he was an appointed member of the Advisory Committee on online security and access of the Federal Trade Commission. He also serves on various state privacy commissions including the California State Privacy Task Force and other initiatives.

Dr. Ponemon is a member of the Unisys Security Leadership Institute (SLI) and the IBM Privacy Management Council. He also holds an adjunct professorship of Ethics and Privacy at Carnegie Mellon University’s (CMU) CIO Institute. Dr. Ponemon is a columnist for Computerworld, CSO Magazine, Dark Reading, and BNA’s Privacy & Security Law Report.

2. Introduction

Network security is important in both the public and private sectors. Our nation’s critical infrastructure is dependent on the secure and uninterrupted flow of sensitive information over the network. This includes our defense systems, air traffic control, local fire departments and rescue services. In the private sector, businesses use the network to communicate, handle financial transactions, manufacture and deliver goods and other processes vital to e-commerce. In short, the network is the conduit for conducting business in today’s global marketplace as well as ensuring our personal safety and security.

The purpose of this paper is to explain the importance of network security and data protection, the risks most organizations face today and how organizations’ can improve their ability to protect their critical information assets. The paper also discusses Ponemon Institute research findings about network and data security methods and technologies. These studies track the perceptions of IT security and data protection practitioners. Included in this paper are observations from a panel of five learned IT security experts.

- Jerry Archer, CSO of Intuit and Distinguished Fellow, Ponemon Institute
- John Reece, chairman and CEO of John C. Reece & Associates and former deputy commissioner of Modernization and CIO of the IRS, and Distinguished Fellow, Ponemon Institute
- Gregory P. Schaffer, CISO, Alltel Communications
- Howard Schmidt, CEO of R&H Security Consulting and former U.S. Cyber Security Czar, former CSO of Microsoft and eBay, and Distinguished Fellow, Ponemon Institute
- David VanderNaalt, Chief Information Security Officer for the State of Arizona and Distinguished Fellow, Ponemon Institute.

3. What is network security?

Network security can be defined as the set of deliberate actions taken by an organization to protect its network and network-accessible resources from unauthorized access and abuse. Network security concerns all devices connected to the network including servers, routers, mainframes, external storage devices, backup devices, desktop computers, laptop computers, wireless peripherals and others.

The arsenal of tools used by IT security specialists to achieve a reasonable level of network security consists of both preventive and detective controls, procedures and enabling technology, such as:

- Authenticating users to the network, including proper provisioning and identity compliance methods
- Ensuring perimeter controls are in-place such as multilayered firewalls, intrusion detection and intrusion prevention systems, and event management tools that monitor suspicious network traffic (including the use of honeypots to trap would-be cyber criminals)
- Encrypting the transmission of sensitive or confidential information between two or more hosts within or outside the network (including transmission over the Internet)

The collection of practices and technologies used to ensure reasonable network security can be a complex and daunting process to manage. Vulnerabilities and threats to a network arise from various reasons, including (but not limited to) the following:

- Security attacks that are becoming increasingly sophisticated and focused.
- Lack of strategic deployment of security enabling technologies across the enterprise.
- Lax policies and enforcement of non-compliance with security requirements, such as allowing end-users to download software that increase network security threats.[1]
- Lax governance over the network security function.
- Emerging state, federal and international privacy and data protection regulations.

4. The changing threats

Security professionals who are responsible for protecting their organization's network need to be cognizant of threats and vulnerabilities that can sorely impact the enterprise. Examples include known holes or glitches in software applications (requiring patches), newly identified viruses or malware attacks, insider threats including negligent or malicious employees, and risks from third-party relationships including the use of outsourcers in the IT environment.

In addition to defending the network in a changing environment, it is important for IT security practitioners to stay more than one step ahead of hackers who may use creative and insidious methods to gain access to devices through insecure points of entry.

During the early days of the Worldwide Web, attacks against corporate or government systems were mostly committed by hackers known as "black hats" who were trying to prove their technical competency. Many of these hackers were high school-aged kids trying to build a handle or reputation.

[1] An example of this issue is the recent controversy concerning the pervasive use of Google's Desktop search engine in network environment, which has been shown to increase the threat of "man-in-the-middle" attacks and cross-scripting vulnerabilities.

The science of hacking has evolved over the years. Now, organized criminal syndicates are sponsoring targeted attacks against organizations on the basis of detection risk and economic benefits. Research by Carnegie-Mellon's CERT shows large organizations that control massive databases containing private financial information or health care records are most likely to be the target for attack. In addition, organizations that outsource data processing centers, call centers or help desk functions to off-shore locations are often targeted.

While recent research shows that insiders constitute a more significant threat for IT security than external threats, indicators suggest external attacks will increase in severity over the next few years. This prediction is based on intelligence concerning organized, tech-savvy criminal syndicates that employ nefarious methods that infiltrate corporate systems. In some cases, these cyber crimes utilize a combination of external and internal attack methods.

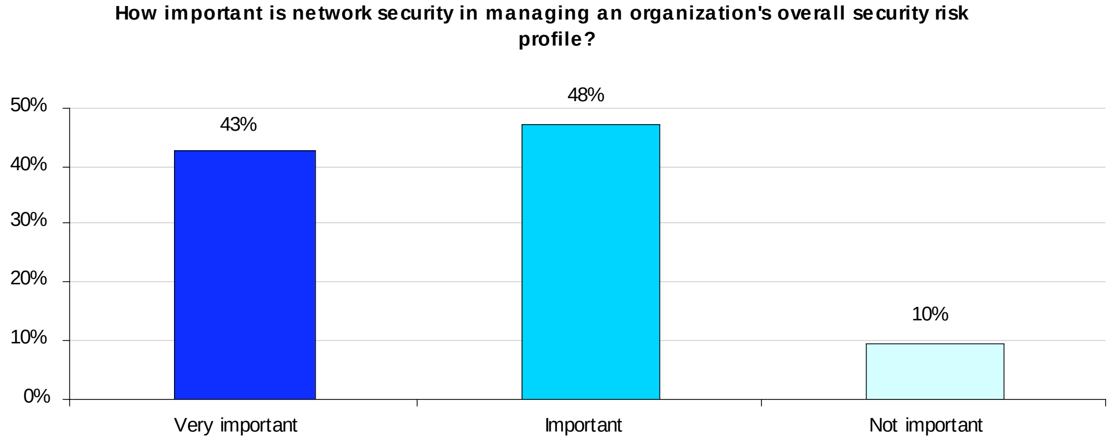
The next section provides important findings about network security from Ponemon Institute research studies of U.S.-based IT security practitioners completed over the past few years.

5. Ponemon Institute research

Since 2002, Ponemon Institute has conducted independent studies about privacy, data protection and information security policy. Presented here are excerpted findings from a collection of recent Ponemon Institute studies showing the importance of network security and data protection in business and government.

The studies were conducted between 2006 and 2007 using scientific survey and sampling methods. The samples recruited to participate in Institute research are experienced IT security practitioners assembled to evaluate leading practices, trends and technologies in the information security or data protection fields. For purposes of this summary, all studies utilized respondents who are employed in the United States.

How important is network security in managing an organization's overall risk profile? As shown below, more than 90% of IT security practitioners in our 2006 IT Security Tracking Study[2] say that network security is either "very important" or "important" to their security mission or objectives within their organizations.

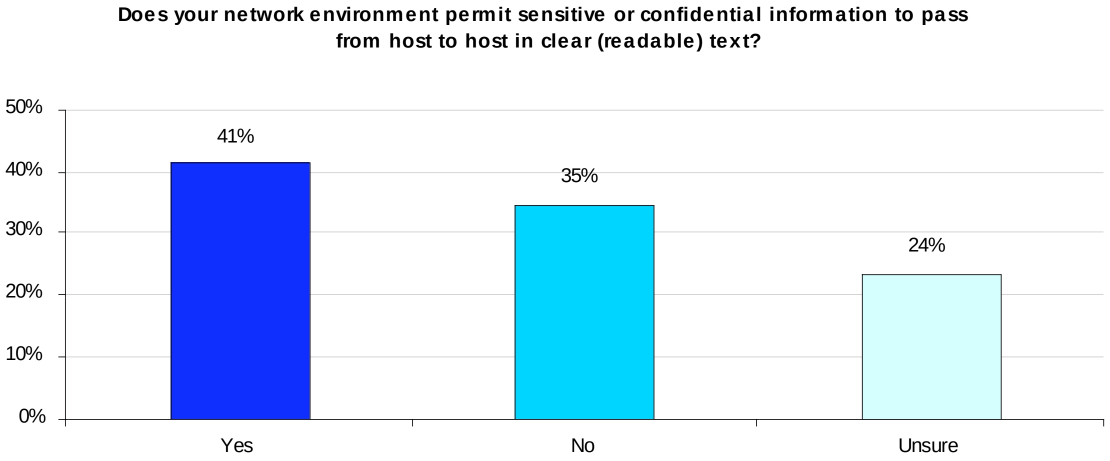


In our tracking 2006 study, we determined that encryption, identity & access management, and perimeter controls (such as multilayered firewalls or intrusion detection systems) are considered

[2] Approximately 1,488 IT security, data protection and privacy practitioner from more than 11 separate studies conducted in 2006 are used to construct the results shown in our 2006 IT Security Tracking Study. For more information, please contact Ponemon Institute at research@ponemon.org.

the most important technical solutions to securing the network. Despite the importance of encrypting sensitive or confidential information over a network, we found that many business and governmental organizations send information in a clear text or readable format.

In one survey we ask, "*Does your network environment permit sensitive or confidential information to pass from host to host in clear (readable) text*?" Results provided below show that the most frequent response by respondents at 41% is **yes**. Another 35% of IT practitioners say **no** about whether their organizations permit clear text traffic when transmitting from host to host. The relatively high unsure response of 24% suggests respondents do not have sufficient control over the organization's IT infrastructure to warrant an informed answer to this direct question.



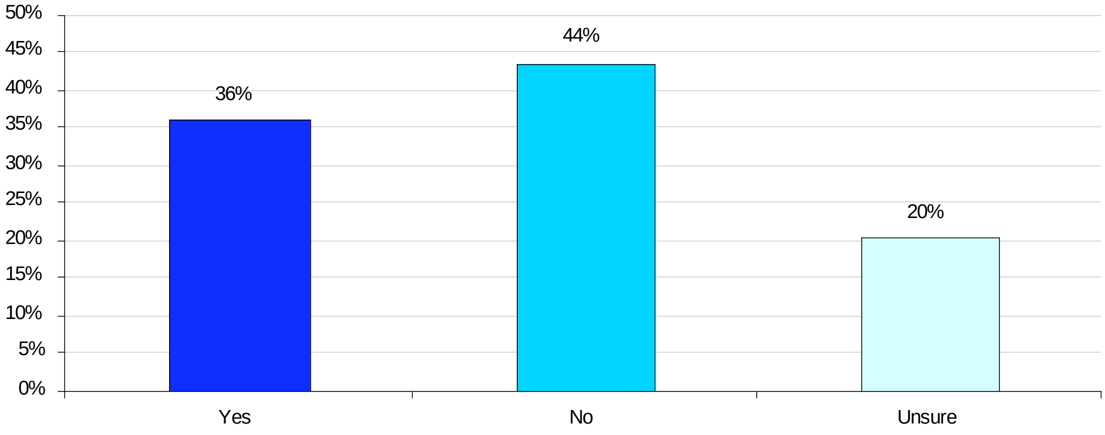
In addition to this survey question, we conducted respondent interviews called "debriefing sessions" to drill down into interesting or anomalous survey findings.[3]

With respect to clear text network traffic, we learned that IT security leaders – such as CISO level individuals – have difficulties enforcing the organization's encryption policies. Hence, while the company's formal policy may demand encrypting sensitive or confidential information in transit to another host or over the Internet, business or application owners routinely fail to comply with this mandate. The most typical reason is that encryption methods are too complex to use properly or encrypting and de-encrypting information causes work productivity declines or system stoppages. Another issue raised by end-users concerns the managing of encryption keys.

In another related survey we ask, "*Does your network environment permit sensitive or confidential information to pass over third party networks in clear (readable) text?*" Results show 36% of respondents say **yes** about their organizations permitting clear text traffic when transmitting over third party networks. Once again, the relatively high unsure response by IT security practitioners suggests respondents do not have controls in-place to inform them about third-party data transfers.

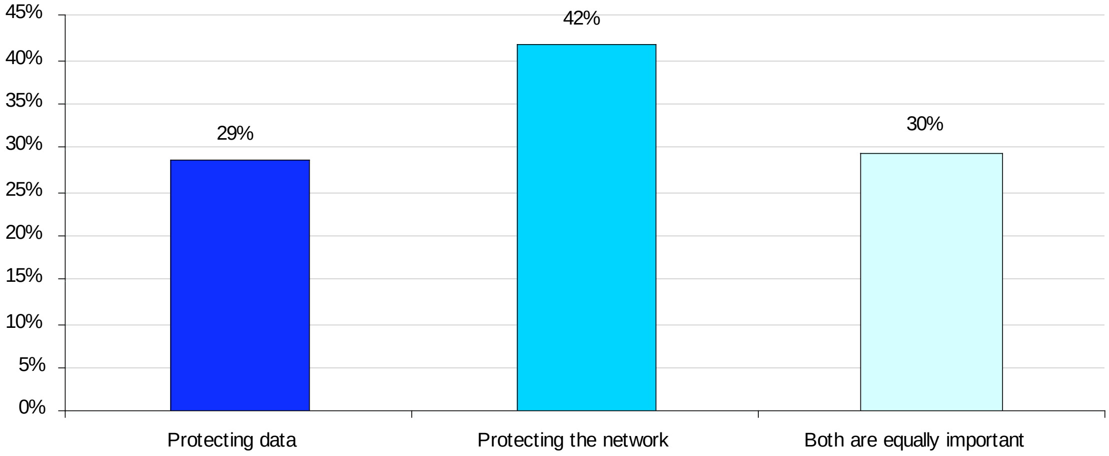
[3] Debriefing is not a scientific research method. Its primary use is to determine the external validity of scientific survey findings. Debriefing is also useful to gain a deeper understanding of a key issue or problem area not specified in the survey instrument.

Does your network environment permit sensitive or confidential information to pass over third party networks in clear (readable) text?

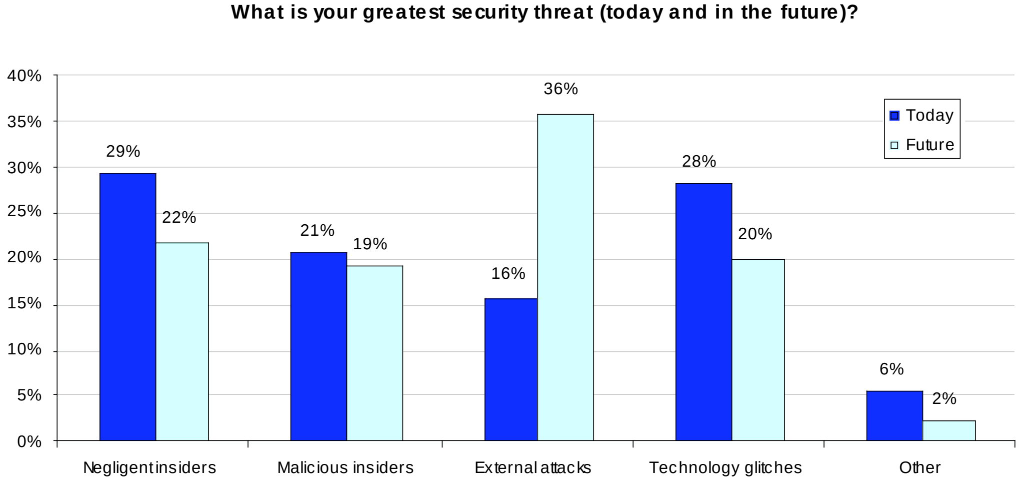


With respect to network security, which protection mission is most important to your organization? According to 42% of respondents, protecting the network is more important than protecting data alone. Another 30% of respondents say that both the protection of their organization's network and the protection of data are equally important in terms of meeting their security objectives.

Which one is most important to your organization?



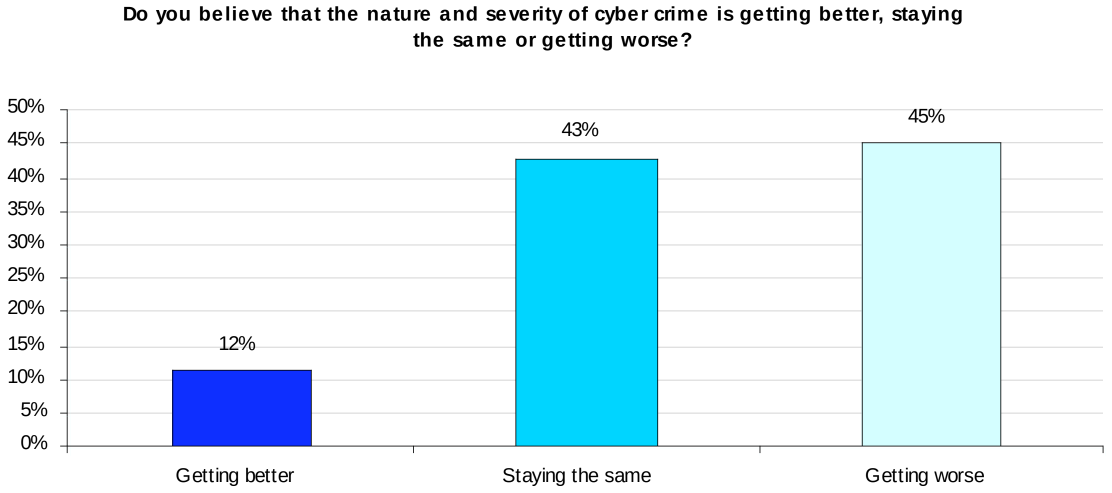
What are your greatest network security challenges today and in the future? With respect to the current state, respondents see insider threats (29%) and technology glitches (28%) as the two most serious threats to their organizations' network security today. Only 16% of respondents see external threats such as cyber-criminals/hackers as their most serious problem. For the future state (defined as 12 to 18 months), however, 36% of respondents see external threats as the most serious security challenge facing their company. This notable rise in concerns about external threats between the present and future state suggests that respondents are bracing themselves for new, sophisticated cyber attacks by organized criminal factions.



Debriefing of selected IT security practitioners about the above question revealed many believe their organizations are not equipped to detect or deter sophisticated attacks that intercept network traffic, especially when information is sent as clear text over the Internet. They also acknowledge that present anti-virus or anti-malware tools are insufficient to stop the projected wave of cyber-crime.

Debriefing interviews also revealed that many companies are starting to see more surgical or structured external attacks through their organization's networks that seek to obtain the most important or profitable sources of corporate information including customer records, employee files, business confidential documents and intellectual properties (including source code, formulae, marketing plans, accounting forecasts, computations, spreadsheets and so forth).

In a follow-up question we asked respondents, *"Do you believe that the threats posed by cyber criminals are getting worse?* " In support of the above findings, only 12% believe that the nature and severity of cyber-crime is getting better. Over 45% of respondents believe that the threat of cyber-crime is getting worse, and 43% are uncertain about how cyber-crime is going to change in the near future.



6. Summary of research findings

Taken together, the above mentioned findings suggest that IT security practitioners are concerned about protecting their network more than they are about protecting their data. They seem to be worried about protecting traffic sent in clear text – especially when sent over a third-party channel or network, but have difficulties accomplishing it. They see the need to encrypt data-in-transit, but acknowledge a lack of resources and organizational commitment to accomplish enterprise-level encryption.

In addition to the above findings, our debriefing of IT security practitioners revealed the following threats to network security:

- The continued practice of sending data in clear text, especially over third-party networks
- The emergence of organized crime in the "IT world"
- The growing complexity of networks, devices and applications on the network
- The desire to enforce and easily manage network encryption

Most important, our findings show that a majority of IT security practitioners are very concerned about the immediate future because of growing threats of serious external attackers to networks and network-accessible information assets. In the next section, we will discuss what our panel of experts revealed about the state of network security and data protection in many organizations.

7. Panel of experts

As noted above, we conducted in-depth interviews with a panel consisting of five noted leaders in the information security profession. This section presents their responses to our questions. We do not attribute comments to any one of the five distinguished individuals in order to preserve their anonymity.

Why is network security important to an organization?

Panelist 1: Network security is extremely important because our critical infrastructure is dependent on data traveling our networks. This includes our air traffic control system, defense systems, local fire departments and rescue services. In business, a technology glitch can have devastating consequences.

Consider the recent case of an airline that wanted to upgrade its systems. A technology glitch caused the computer system to fail resulting in a massive disruption of the transportation system. Planes couldn't fly because passengers couldn't be boarded. And, it wasn't due to air traffic control— it happened because of an organization's inability to manage the upgrade and the network crashed. The disruption also had serious business implications because the electronic ticketing system was down and it was impossible for passengers to be ticketed.

Panelist 2: Network has become a critical piece of the IT infrastructure for most businesses and governmental entities. Without a secure and reliable network, a business won't run. If nothing else, businesses rely on telecom networks for conducting normal business such as communicating via e-mail, processing credit card transactions, or sending critical business data. There has been a dramatic change in the importance of the network. Twenty years ago, our only focus was protecting the data. Now it is imperative that you protect the network infrastructure in order to protect the data. Tools such as encryption have become more convenient, making it easier to secure confidential data transfers, especially over third-party or Internet channels.

Panelist 3: The network is the conduit for conducting most electronic business transactions. If you defend the network you defend the data. While many security practitioners focus on data at rest, I would rank network security as the most important security object we [security professionals] should be concerned about.

Panelist 4: The network has become increasingly more important over the past few years because of network expansion, including Internet and extranet activities. In essence, commerce doesn't happen unless the network allows it to happen. This means the movement of both hard goods and soft goods can't occur without a well-functioning, reliable network. The network is even more important going forward as companies will use electronic tagging and RFID to secure the movement of physical products.

Panelist 5: Security has a hard time keeping pace with end-user requirements for fast and reliable network transactions. While network security is one of the most important goals for IT security, data protection and privacy, it often gets little attention until a disaster or catastrophe hits.

What is the greatest threat (negligence, temporary or contract workers, malicious insiders, external hackers, technology glitches)?

Panelist 1: If network security is poorly managed it puts the entire business at risk. AMEX in the late 1980s realized that a disruption in services for every minute cost the company $1 million because people who could not use their American Express card would swipe their Visa or Diners Club card. That loss would be even greater today. It is important to have robust capable systems that make nearly perfect network security part of the infrastructure. While I worry most about the insider risks that disrupt the network, external attacks by the proverbial "bad guys" is definitely an increasing threat.

Panelist 2: Frankly, it doesn't matter who the perpetrator is, the focus needs to be on remediation – or the consequence of lost or stolen confidential information. In my experience, the negligent insider poses the greatest threat; however, external threats should not be taken lightly. I also see external attackers such as Nigerian or Romanian cyber criminals as getting better or smarter. Over time, external penetration of insecure networks is quickly becoming a major enterprise in certain developing economies.

Panelist 3: The basic flaw in network security is permitting companies to send sensitive or confidential information over unsecured channels, especially third-party network channels. I believe that much of this risk can be mitigated if companies start to use encryption – especially for data that is considered critical to business operations such as customer records.

Panelist 4: As networks expand, more temporary and contract employees need to be connected. In addition, many end-users demand immediate connectivity from mobile devices. Today, the real threat isn't a malicious attack, but mistakes that ultimately lead to the loss of information assets. In the future, however, the threat is likely to shift back to external attackers who are using more sophisticated methods to intercept network traffic.

Panelist 5: I'm most concerned about organized cyber-crime including cyber-terrorism. I believe that IT security needs to stop being complacent about the rash of small scale network attacks seen today by most businesses. Clearly, we can defend ourselves against most external threats using conventional tools. But, cyber criminals are getting much smarter and more insidious. We need to worry about the attacks we don't see or know about today. My gut tells me things may be a lot worse than we believe it to be – in essence, the calm before the storm.

What type of data is more vulnerable when traveling through networks as clear text?

Panelist 1: Data risk depends on your business model. As a starting point, you need to categorize data as confidential or non-confidential. However, you need to be aware that the non-confidential can become sensitive if you begin to combine different data sources. For example, clever thieves can look at pieces of publicly available data such as a person’s date of birth and home address, and combine these data elements that put you at serious risk. This problem is getting much worse with all the public and non-public information that can be gathered over the Internet using Google and social networking sites.

Panelist 2: The Holly Grail of information is intellectual property. Fortunately, most of this type of information is stored in secure, off-network locations. For purposes of normal network traffic I am worried most about customer information – especially credit or debit card transactions.

Panelist 3: The risk of intercepting confidential business information such as accounting reports or strategic plans is negated by using encryption. Companies should organize their data traffic according to priority or risk level. Every transaction concerning high priority data transit should be encrypted, even if this results in system degradation or other end-user hardships.

Panelist 4: All data, whether trade secret or publicly available information, should be treated as a business asset. I believe that classification schemas oversimplify the basic requirement that it is never acceptable to lost or leaked business information. The transfer of confidential information as clear or readable text is an unacceptable practice that should be outlawed by company policy.

Panelist 5: In my company, the protection of personally identifiable information about customers, consumers or employees is the most important data type. We focus on lost or stolen PII because of all the breach notification requirements that are very costly to a company’s reputation when made public.

What is more important, protecting the data or protecting the network?

Panelist 1: It is a “hand in glove” type question — the data itself is the currency of the digital world so it needs protection but the network moves the data so it must be secured as well.

Panelist 2: Both. Network is critical to the business’ infrastructure. We use the network to conduct business and transaction data travels the network.

Panelist 3: In my mind, securing the network is most important.

Panelist 4: Protecting network assets is the first step toward reasonable data security. Once the network is protected, a company can focus resources on data at rest. So, I see both as equally important.

Panelist 5: It depends on the company and its business model. In most network-driven IT infrastructures, network security is the overwhelming dominant priority.

What is the value of protecting the network to an organization?

Panelist 1: Number one – avoiding business disruptions and inconvenience to consumers.

Panelist 2: The goal of having a secure network forced my company to have backup processing capability so that the network was never down. As a competitive advantage it was good to be able to tell customers that we have an intrusion detection system that protects their records. Because of trust in my bank that my transactions are protected I will do my banking online from home. I can do more banking from my home than when I physically went to my branch. This means more profit for the bank and more convenience for me.

Panelist 3: The most important value is to minimize inefficiencies resulting in work stoppages and other end-user inconveniences. This helps to build trust and confidence among end-users and the corporate IT function.

Panelist 4: Frankly, it is impossible to maintain channel partnerships if your business partner can't depend on the security of your network. Good network security is essential to building confidence. Another way to look at the value question is to consider the consequences of not securing network traffic. A string of network failures can put a company out of business.

Panelist 5: The value of network security depends, at least in part, on business focus or industry sector. For instance, retail banking organizations must take significant steps to defend networks in order to do any financial transaction. Beyond regulatory requirements, the failure to operate a secure network would have devastating consequences for any financial service company.

What are the elements of good network security?

Panelist 1: As a starting point, it is imperative for a company's leadership to fully understand and support network security. It requires good policies that are strictly enforced. There is a need to validate or monitor the policies because employees will deliberately circumvent policies that are not enforced.

Is there accountability for protecting business and IT processes in the organization? Is there someone making sure the DNA of the business is secure? Realize that bad things can happen to any network no matter what protections exist so it is important that a good response mechanism is in place.

Panelist 2: Good network security requires robust technology. As an example, my organization had a denial of service attack but security was so well designed that the network was up in seven hours. Any organization that did not have top of the line technology would have been down for weeks. Make sure the network is patched to the proper levels and that the hardware is current and vendor maintained. The one agency that was not up had hardware so old that the vendor hadn't supported it in years. Today an internet year is three months. It is incredibly important to have identity and access controls, intrusion detection systems, spam filters and encryption.

Panelist 3: It starts with leadership across the enterprise. Network security can't be managed in fragments or pieces. The control of networks and network-assessable resources requires holistic execution. An organization must have a response plan. It is critical for all organizations to know the tactical steps it must take to restore a network after it has been hit or attacked.

Second, it is about securing access rights on a "need to know" basis. Third, it requires all devices, including wireless or portable devices, under control at all times. Fourth, it requires all data-bearing storage devices taken off-network to be secured. Finally, it requires constant vigilance and monitoring.

Panelist 4: I'm a believer in better technology is required to solve the network insecurity problem. Accordingly, encryption is the way to go. As mentioned, don't allow readable text to be sent over networks.

Panelist 5: Good network security is about four things – people, process, technology and policy. Achieving network security is a balancing act for all four components.

Convergence is creating a new set of challenges for network security and how to conduct business that is entirely secure. The solution is to blend encryption with smart cards biometrics and some form of analytics profiling. One large financial services firm has a profile on each cardholder. For example, what are the cardholder's typical transactions, purchases and creditworthiness? All done to determine you are the right person making a purchase. I can see some form of positive profiling for all network security.

Most everything will soon be encrypted even at the chip level. The issue is what do you do beyond encryption? Physical security is equally important. Whatever methods of access information you want to have pretty much the same identifiers.

Does your network environment permit clear text to travel over the network? If permitted, why?

Panelist 1: Unfortunately, we do permit clear text data transfers. It doesn't make sense anymore given the network solutions available in the marketplace, but some will say that encryption causes the network to slow down.

Panelist 2: Yes, we permit clear text in some instances. The main reason for permitting clear text rather than encryption is to use content filtering for certain data streams, especially over third-party or Internet channels.

Panelist 3: Typically, we do it because the end-user doesn't think the encryption and de-encryption of documents is worth the effort. The culture is starting to change given the risk of data loss and breach notification. Also, Sarbanes-Oxley 404 requirements put pressure on the business and application owners to secure data transfers.

Panelist 4: No comment.

Panelist 5: We are striving to stop transfer of confidential information, especially over third-party channels. The reality is that this is a very slow process that no one party wants to own it.

What are the elements of bad network security?

Panelist 1: First and foremost, it is not having a response plan. Incident management is important.

Panelist 2: The indicator of bad network security is a lack of top level support. Real resources are required to get the job done. Companies need to invest in the right technologies and tools.

Panelist 3: An indicator of bad security is being aware that sensitive or confidential information is being sent over insecure channels as readable text.

Panelist 4: In my experience, not knowing all devices connected to the network is a sign that the process is out-of-control. Unfortunately, having a "full view" is increasingly difficult with the onset and widespread use of wireless portable devices. Everyone wants to be connected, but very few are thinking about the security ramifications of insecure connectivity.

Panelist 5: Bad network security is a lack of leadership and backbone. The end-users want connectivity and convenience. They aren't worried about network failures resulting from systemic attacks. Sometimes it is important to say no, at least until you figured out the security implications of more connectivity.

8. Recommendations:

How do you protect the security of both your data and the network? Here are recommendations from our panel of experts:

1. Take a holistic approach. An organization needs to protect both the data and the network because they work hand-in-glove. The data itself can be considered the currency of the digital world so protection is critical. The network moves the data so it must be secured as well.

2. Conduct regular risk assessments. Understand what types of data are traveling your network. Typically, data can be categorized as confidential or non-confidential. Take appropriate steps to protect confidential data but be aware that clever insiders or thieves can access your network and take pieces of data, combine them and as a result put your organization's sensitive data at risk.

Risk assessments should take into consideration an organization's business model. First, analyze what types of data are most confidential if you are a retailer, bank, healthcare provider or hospitality business. Second, after classifying the sensitivity of your data you need to consider who should have access to data and how the data should be secured as it travels from point to point on the network. Risk assessments are critical to understanding how resources should be allocated to protect the network.

3. Accountability must occur at the leadership level. How well does the leadership understand and support the importance of protecting the network? Is there someone accountable for making sure the DNA of the business is secure? Without leadership's commitment to security, it is difficult, if not impossible, to achieve the recommendations listed here.

4. Assemble a network security risk council. The council should be comprised of representatives from the following areas of an organization: security, legal, human resources, privacy, information technology, internal auditing and operations. The purpose is to determine what would be the greatest threat to the business if the network went down. This risk cannot be decided by the IT department alone. Risks are dependent upon the environment in which the business operates.

5. Ensure enforcement of network security policies. It is important to validate that policies are being followed and employees are in compliance. Employees can deliberately circumvent policies. Therefore, it is important to make sure that mechanisms are in place to detect non-compliance and punish negligent or malicious employees.

6. Invest in robust and up-to-date network security technologies. Make sure network is patched to the proper levels and that the hardware is current and vendor maintained. Blend encryption with smart cards, biometrics and analytic profiling. Encrypt everything even at the chip level. Network partitions in order to be able to select the "tunnels" you want to protect. Scan the network to know where every device is. An alert system should be built into the network to shut down devices.

7. Have an incident response plan in place. Bad things can happen to good networks. While technology can help protect the network, it is important to have plans in place to deal with network disruptions.

9. Conclusion

In this paper we have discussed the importance of network security and the challenges faced by IT professionals to address changing threats to the network and sensitive data. Given the consensus that network security is a very important component of an organization's overall security profile, we believe the recommendations offered by experts in this report are practical and useful. In general, organizations should seek opportunities for the greatest overall increase in network security for the least amount of effort or expense.

Among the tools available to organizations, we believe that encrypting network traffic is a first line of defense for protecting sensitive or confidential information sent over third party networks, thus reducing some of the most significant security or privacy-related vulnerabilities due to negligent employees, unstable operating systems and other potential causes of a data loss or theft.

It is interesting that one of the findings from our research is the perception that encryption is viewed as too complex, expensive and not compatible with some other networking and security practices. Our experts believe this is not grounded in fact and often based on an outdated notion about network encryption. In my opinion, there have been enormous strides in making encryption solutions for data in-motion and at-rest painless for end-users. Many of these solutions are cost effective, thus yielding a strong ROI or TCO result for business and government organizations.

Respectfully,

L.A. Ponemon

Dr. Larry Ponemon
Chairman