Cyber Exposures - More than the Technical

Douglas A. Nagan
President, Nagan Research Group LLC

Initially, when faced with threats, man had to choose between 'fight' or 'flee'. In these times, we have many more choices because, along with the increased number and sophistication of threats, we have created improved strategies, technologies and techniques to address them. In the cyber area, as you well know, the threats include viruses, hackers, trojans, phishers, and other numerous malware creations. There are many efforts underway to combat these threats. Unfortunately we also see many failures that share the following characteristics:

- **Myopia** - a focus on the obvious to the exclusion of other potential threats. A good historical example is the Maginot Line. The French series of fortresses and defenses created in the 1920's and 30's to prevent a German Invasion. The French did not create a defense on the Belgium border because Belgium posed no threats. This left them totally unprepared when the Germans went around the Maginot Line and invaded through Belgium. This failing to recognize broader strategic risks is not confined to mid-twentieth century French myopia, but is alive and well in organizations today. We see organizations installing the latest secure firewalls and then letting staff connect their smart phones directly into the protected network – commonly called 'Bring Your Own Device (BYOD)', thus by-passing their own security 'Maginot Line'.
- **Willful, Head-In-The Sand, Ignorance** – the belief that "it won't happen here." Generally founded on the concept that we are too small, or pose no threat so we will be spared. The mistake here is to think that the malware activists are looking for some specific asset. The truth is that many are just looking for vulnerabilities that can be compromised. Many are interested in proving they are smarter so being small or posing no threat is irrelevant. In the cyber environment all are potential prey, none are spared.
- **Human Failings** – a combination of myopia, ignorance and just plain mistakes. Example abound: lapses in vigilance (not encrypting sensitive information), carelessness (leaving thumb drive in taxi), and sheer laziness (using default settings and simple passwords).

The current environment

The myopia, ignorance, and failings are all present in today's cyber environment. While there are multiple efforts underway discussing technologies, techniques, and tools to address cyber exposure organizations continue to leave themselves exposed. What do we mean by 'exposed'? Here are some recent and sobering findings:

Verizon's 2012 Data Breach Investigations Report found that victims fell prey because they possess an exploitable weakness.

- 97% of breaches were avoidable through simple or intermediate controls
- 96% of attacks were not highly difficult

Symantec 2011 Cost of Data Breach Study found the largest root cause of data breaches was negligence (39%)

When RockYou was hacked in 2010 32 million passwords were made available and researchers, as reported in the NY times on January 21, 2010, found the following:

- Nearly 1% used '123456' as their password with second most popular '12345'
- Others in the top 20 included: 'password', 'qwerty', 'abc123', and 'princess'

- 5,000 passwords made up 20% of the 32 million passwords.

In the June 26, 2012 issue of Baseline magazine a survey of Bring Your Own Device (BYOD) usage found the following:

- 74% of respondents already use their own mobile devices for work
- 36% have or would contravene a policy banning personal devices at work

All this adds up to making the hacker's job easier.

In view of the continuing growth of malicious cyber activity, Nagan Research conducted a survey in early 2012 to gain some insight into how individuals are addressing their personal cyber risk. The objective was to gain an overview of basic technology use, behavior, and protection. The following summarizes our findings.

The usage of Wi-Fi, social networks, on-line services, and memory sticks to transport data means that the majority of individuals are exposed to a wide range of potential cyber hazards.

- Over half the responders (53%) use Wi-Fi when travelling
- Most use social networks, many more than one (LinkedIn 69%, Facebook 44%)
- A vast majority use some on line banking services (89%)
- Buying on-line is a normal way of life (78%)
- Memory sticks are used by half (50%) to transport information

They are not rigorous in protecting their personal sensitive information including social security numbers, bank account numbers and credit card information.

- Less than half only provide such information to verified secure locations (47%)
- Only 8% do not provide such information to any on line source
- Only 19% encrypt sensitive information on their personal devices

They rely on historically proven approaches to protect themselves

- Firewalls 75%
- Recognized Protection (Norton, McAfee, etc.) 86%
- Spam filters 72%
- Passwords they create 81%

They make little effort to be prepared for adverse consequences

- Only 35% perform back-ups on a regular basis
- 23% back up irregularly or not at all
- Over two thirds (69%) do not use or have any insurance or identity protection service

The following table summarizes the seriousness of the individual lack of attention to cyber security. When we classified the responses using a simple 1 (no, or negligible risk) to 5 (extreme risk) rating for each question then summarizing for the level of exposure , no respondents had low personal cyber exposure and the majority had either significant or serious personal cyber risk exposures.

Low	0.0%
Moderate	38.5%
Significant	51.3%
Serious	10.3%

Individual Cyber Exposure

The data above shows that, while cyber risk remains a real and potent threat, it is obvious that individuals are not taking appropriate measures to protect themselves and their assets.

Adding improved protection and insurance represents the simplest approach, but individuals are unlikely to take even these precautions until cyber risk becomes more urgent and more personal. In the short term this implies that the best approach for individuals is to make sure they take strong precautions (such as the encryption of sensitive information, perform regular scheduled back-ups, only use secure verified on-line sites, and have insurance or a protection service) leaving the less protected to the cyber predators.

This individual approach to cyber exposure may carry over into one's professional life unless the individual is in an organization fighting cyber intrusions on a regular basis such as banks and credit card processors. Sloppy, careless and negligent personal security habits will likely translate into similar behavior in the workplace. This may explain the lack of enthusiasm in organizations to aggressively address cyber exposures since their employees, in their personal lives, are not paying attention either.

In summary while the current environment has many quality tools to address technical cyber exposures, too many organizations do not have a strategic disciplined approach to their cyber exposures and because many individuals in responsible positions who should know better, treat their organization's cyber security as they do their personal cyber security.

Cyber exposure beyond the technical

The article 'Common Misconceptions in Computer and Information Security', from the June 2012 issue of Computer (page 102) has among the misconceptions detailed 'Security is a purely technical endeavor'.

To better understand this misconception, consider the following examples of non-technical cyber exposures.

- Legal – Examples abound in this area. We will provide three to give the flavor. First there is a great rush to use cloud computing services for the obvious cost and capacity issues, however, the agreements with the providers rarely provide for liability protection and data loss if servers are legally sequestered. When Megaupload's service was taken down by the United States Justice Department, many legitimate companies lost access to their legitimate corporate data and have yet to get it back a year later. Second few technical organizations have counsel review the use of trademarks, and copyright material on their web sites. In a recent Google Transparency Report (June 18, 2012) Google received over 1.8 million requests to remove specific URL's. In 2010 YouTube won a summary judgment over Viacom in a massive copyright infringement case. The parties spent over $10 million in legal fees. Third who monitors postings on social media to make sure there are no postings that pose legal liabilities? The United States Army is so concerned they have updated the Uniform Code of Military Justice to outline permissible use. It can best be summed up as: 'If you would not say it in formation or to your leaders face - then do not say it'. The punishments can be severe including court marshal. Commercial organizations cannot court marshall their employees but they still need to make it clear what they consider proper usage of social media and what they will do if these usages are not followed. While there are many more examples, these should suffice to make the point that there are many unique legal exposures that arise from cyber technologies.
- Compliance – In the compliance arena, there are the federal regulation such as: Sarbanes Oxley, Basel II & III, Red Flag Rules, OSHA, PCI, and HIPPA to name a few. Each brings requirements that must be met that have little or nothing to do with technology yet require technical decisions, such as how to encrypt personal information in health files, that have great impact on meeting the requirements. Once you have fought through the thicket of federal regulations you now have to

deal with the states which are beginning to get into the act. Many are setting up their own regulations concerning what organizations have to do when personal information is compromised. For example a Massachusetts General Hospital employee took some work home but left 192 paper billing records containing detailed personal health information on the subway. The institution was fined $1 million and subjected to a three year oversight program.

- Policies and Procedures – It used to be that the only documentation that IT management had to worry about was operating procedures and user manuals. Today they have to be concerned with helping create policies regarding the protection of information assets such as relevant and enforceable protocols for Facebook postings.
- Human Resources (H/R) – Among H/R's historical functions is as the coordinator of organization wide training. This role is expanding to include securing organization information assets, the use of social media in hiring, and procedures for disciplining those who expose organizational confidential information.
- Intellectual Property – With the access and easy portability of information organizations have to step up activity to protect their own intellectual property and not to allow the misuse of others intellectual property on their equipment. For example this could include the copying of white papers, posting of proprietary links, forwarding proprietary information. The ease of the copying and transporting information makes it extraordinarily easy to transgress on other intellectual property.
- Human Behavior – The failings of our species are all too well known and the capabilities of technology magnifies incidents. What is needed, if one wants to address cyber exposure, is constant training, monitoring, an understanding of the exposures that can arise through inattentiveness, and an organization culture that provides positive feedback in the management of cyber exposures.
- New Technologies – Recently we have seen the impact, and un-intended consequences that new technologies can have on organizations. Think of the smart phones, tablets, social media and cloud computing. Each brought an ease of use, much improved capabilities, ubiquity, low cost and at the same time opened organizations to unexpected vulnerabilities and many did not even realize the exposure until an event occurred.

The above listed items exemplify the breadth and range of the real and increasing non-technical cyber exposures out there. Each one brings with it potentially substantial exposure for any organization.

The high risk implications of ignoring the non-technical cyber exposures
The prior examples show that there exists a wide range of cyber exposures beyond the technical, and organizations and individuals are not fully engaged in preventative actions. When combined, we have a recipe for disaster.

This raises the following questions:

- Do you understand your full range of cyber exposures?
- Have you allocated resources and set priorities to adequately address the full range of your cyber exposures?
- What have you done to minimize the potential of human failings?
- Do you have contingency plans in place to deal with a cyber event?

The solutions may not be obvious but neither are they optional.
At the organizational level, several things need to be done.

1 – Each organization needs to gain an appreciation of <u>all</u> their cyber exposures. There are several ways they can do this. One way is to create a high level task force that needs to include representation of IT management, counsel, HR, and Audit to create, document and

communicate all cyber exposures. An alternative is to use outside experts that can assist by performing cyber exposure assessments. Additionally there are services that provide the means to capture and summarize an organization's cyber exposures in a timely and economical manner.

The organization may have existing structures in place, such as an Enterprise Risk Management Program that the cyber effort can integrated into. No matter what approach is used, the organization needs to address the following exposure areas:

- **Cyber Activity**: This is an overview of all the cyber activity across your entire organization not just in the technology departments. Who accesses what data using what technologies and are they secure? What technologies are in use?
- **Privacy:** Does a senior level management official exist, whose responsibility it is to ensure that personally identifiable information, proprietary organization information, or other sensitive information, is not released, accidentally or intentionally, without the proper authorization and safeguards?
- **Computer Systems**: Who is responsible to ensure that the organization's computer system(s), networks and other applied cyber technologies are secure?
- **Legal**: Does the organization and cloud computer vendor(s), if used, have cyber liability insurance? Has the organization established intellectual property (IP) or compliance procedures across the entire organization and its many departments and individuals, including each of the following:
    - periodic IP audits accomplished by legal staff or outside counsel, or both;
    - training of employees regarding copyright and trademark issues;
    - acquisition of all necessary IP rights via licenses, releases or consents?
- **Security Policies and Procedures:** Has the organization established responsibility for records and information management compliance with an experienced records/compliance officer holding a dedicated position?
- **Social Media**: Does the organization use, or permit management, employees, contactors or vendors to use, any social media platforms, including, but not limited to Facebook, Twitter, foursquare, LinkedIn and MySpace, utilizing equipment furnished by the organization for any purpose?
- **Compliance**: At the most basic level the organization needs to be aware of the federal regulations they are subjected to including, but not limited to: Sarbanes Oxley, Basel II & III, FTC Red Flag Rules, HIPPA, and Dodd Frank. Beyond that what is the organization doing in response to a number of state laws that require the establishment of a proactive procedure for determining the severity of a potential data security breach and for providing prompt notification to all individuals who may be adversely affected by such exposures?
- **Cloud Computing**: Has the organization explored and resolved the following issues with their cloud computing provider:
    - whether the organization's data will be stored only in the United States to resolve any jurisdictional issues in the event of a dispute with the provider;
    - the financial stability of the provider, including reviewing third party audit reports of the provider's security and privacy practices, the results of internal audit reports, a copy of the provider's Disaster Recovery/Business Continuity plan and the results of the latest comprehensive test of this plan?

Given the magnitude of the potential cyber exposures the highest level of the organization should be aware and participate. Unfortunately as stated in the Carnagie Mellon CyLab report 'Governance of Enterprise Security – CyLab 2012 Report'- dated May 16, 2012: ' 57% of respondents are not analyzing the adequacy of cyber insurance coverage or undertaking key activities related to cyber risk management to help them manage reputational and financial risks associated with the theft of confidential and proprietary data

and security breaches.' An organization that wants to manage its cyber exposures needs to be in the 43% that are paying attention.

2 - The organization needs to treat and manage cyber exposures following a disciplined process that includes the following steps.

- Develop the level of exposure the organization is willing to tolerate beyond which it needs to find alternatives. This is generally called developing the organizations risk appetite. There is no escaping the potential for risk, however it is possible to decide what risks to accept, what risks are worth minimizing, what risks should be transferred (i.e. – insured), and what risks will the organization ignore.
- Measure and size potential impact of the exposures found in step 1. Benchmark data can be gathered from studies such as the Ponemon Institute 2012 Cost of Cyber Breach Report .
- Develop a plan as to how to address the organizations cyber exposures. Use the information gathered in the steps above to establish priorities and allocate resources aligned with the organizations strategy..
- Develop and implement the appropriate and necessary security policies and procedures. Make sure they are distributed and adhered to via audits
- All employees, vendors and consultants need to be trained in expected cyber security policies and procedures. This training needs to be updated on an annual basis to reflect the changes that will occur.
- Adherence to the policies and procedures must be tracked by the organizations audit department.
- Create implement and distribute a set of metrics describing the organizations cyber exposures, incidents and activities.
- Response plan – Create, implement and test a plan that details the necessary actions should the organization experience an event

On a Individual level, where we have seen much of the cyber exposure arise, the following needs to be done

- Education raising awareness of the issues and magnitude of the potential cyber exposure and how they need to behave to minimize the cyber exposure they expose the organization to.
- Distribute and provide cyber protection to all devices that can connect to the organizations networks. Including BOD if that is deemed appropriate/
- Measure and monitor usages to verify that proper security procedures are being followed and discipline where they are not.
- Finally make part of their compensation dependent upon adherence to the organizations policies and procedures.

These steps will not eliminate all cyber exposure, but they will certainly lessen the exposures.

In summary

- Organizations need to become aware of and address the full range of their cyber related exposures. We need to encourage better awareness of the mundane as well as the technical
- Individuals need to become more aware and disciplined.
- The technical community needs to become more involved in the strategic approach to cyber exposures and realize that we are all part of a larger challenge