Volume 24, Issue 4 – December 2015

DRIE Digest

Disaster Recovery Information Exchange

157 Adelaide St. West, PO Box 247, Toronto, ON M5H 4E7 Call: 647-299-DRIE Website: www.drie.org

IN THIS ISSUE

IT Security Policy

Proven defense for cyber attacks

Vito Mangialardi
Allstream
Director Business Continuity Management and Security Services

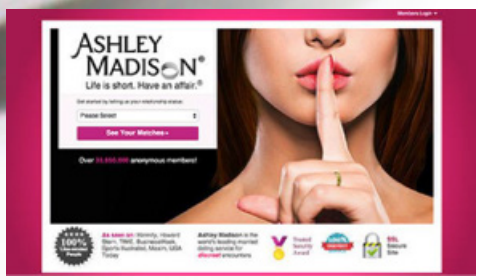
Business and operating environments are changing on a daily basis. Once upon a time, critical business information was generally associated with financial records which were kept protected on paper ledgers in a fire proof safe. Today it is a different world when we consider e-commerce, 24/7 hours of operations, partnering with vendors and suppliers, increased data storage, customer demands, and privacy of information. Couple this with the growing reliance on automation and technology; not to mention emerging business threats (cybercrime, acts of terrorism, natural disasters, pandemics, severe weather and climate change) bring into focus the importance of information security during normal operations. It is something that becomes even more important when we are faced with ensuring business continuity of operations in any kind of business disruption or disaster.

People use Information Security and Cyber Security interchangeably. They are two distinct and important definitions:

- Information Security (IS) is designed to protect the confidentiality, integrity and availability of computer system data from those with malicious intentions. Confidentiality, integrity and availability are sometimes referred to as the CIA Triad of information security.
- Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, the term security implies cybersecurity.

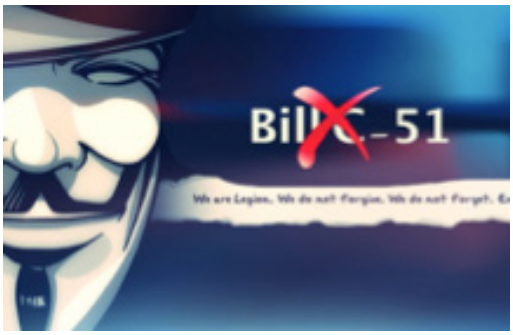
Information and information systems are critical to almost all businesses today. C-level executives now, more than ever, are embracing the concept that computer information security is a fundamental business process required to maintain the integrity of the business, and uphold customer confidence and trust.

What have we learned regarding impacts from recent cyber crime incidents?



Ashley Madison was the target. They are a Toronto-based company, which offers a unique discreet service to consenting adults for a fee. They received fair warning, that if they continued operations a group was planning to breach their security. Eventually it occurred and Ashley Madison has to confess that client personal information was released to the public (and more than once). The information released, as you can imagine, had life changing results ,due to the nature of the services provided by Ashley Madison.

This past June 2015 **The Canadian government** became a cyber-attack target of the activist group called "Anonymous 'in response to Bill C-51. The result was a surgical struck denial of service (DDoS) attack on the network, which caused the website to be impaired for hours. While no loss of sensitive information occurred, the inability for users to access the site was disruptive and with that the primary directive of Anonymous was achieved.



Another good case study to learn from is one of the largest business retail data intrusions in U.S. history. In December 2013, Target was impacted when malware was set in place to collect and move stolen credit card and debit numbers (approximately 40 million numbers) at the company's 1800 retail locations in both US and Canada. At the point of transaction when the cashier would process the payment 'via the credit swipe' the malware would take over and perform an extraction of data. This event altered the company's reputation dramatically and has proven a PR nightmare to recover from in the public eye.

Data Breach
TARGET

A cyber security incident may fall under into several categories. The following are some key examples:

Denial of Service

- An attacker sends specially crafted packets to a Web server, causing it to crash.
- An attacker directs hundreds of external compromised workstations to send as many Internet Control Message Protocol (ICMP) requests as possible to the organization's network.

Malicious Code

- A worm uses open file shares to quickly infect several hundred workstations within an organization.
- A business might receive a warning from an antivirus vendor that a new worm is spreading rapidly via email throughout the Internet. The worm takes advantage of a vulnerability that is present in many of the organization's hosts.

Unauthorized Access

- An attacker runs an exploit tool to gain access to a server's password file.
- A perpetrator obtains unauthorized administrator-level access to a system and the sensitive data it contains.

Inappropriate Usage

- A user provides illegal copies of software to others through peer-to-peer file sharing services.
- A person threatens another person through email.

Insider Information Threat

- An insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems

Scope of Computer information Security Policy

The use of a policy is the best approach to a Guideline document.
A Policy is typically an organizationally adopted document associated with an overarching operational interest that defines the specific requirements that must be adhered too (Thou shall do). In this case the focus is on the information technology framework of applications, business systems and elements including the supporting connectivity layer (the networks). Structured Policies are easier to implement if they include associated standards and or guidelines.

A Standard, used and associated with the specifics of the Policy, defines details such as 'how it is used and under which circumstances'. A Guideline on the other hand is much more flexible and based on some industry best practice.

Understanding where such a Security Policy is best focused with an organization is similar to Business Continuity Planning – Business Impact Assessment (BIA)—however in this case it is 'technology focused'. First establish the criticality and risk exposure of your IT environments by documenting responses to the following questions:

- What constitutes a complete inventory of IT technologies, processes and practices that exists to support or operate the business networks, computers, programs and data?
- What are the required Information Security (IS) requirements that must be in place to ensure the information integrity of your IT environments?
- If you Measure the "we must have"' to what "we already have," what is the plan to address the gaps?
- What is the financial and operational impact to the business if a Cybersecurity situation presented itself? Example: where data (information) were lost or corrupted, and your website or IT system compromised.

When it comes to personal information consider the following which should form part of a Security Policy

- Personally identifiable information (PII), or Sensitive Personal Information as used in US privacy law and information security, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

A good practice to include in the Security Policy is where internal processes may be weak and have the potential for a breach. Special attention should be paid to instances where personal information may be at risk. The media is very fond of bringing to light any business failure to protect PII. This is one instance where "not all press is good press". The media attention from this type of breach brings a tsunami of risk to your business brand and consumer trust. Organizations with a significant amount of PII (telcos, insurance companies) could potentially be ruined by a significant data breach. Ashley Madison is a perfect example of a business that is highly unlikely to survive their security breach incident of PII. For companies that are considering how strict to make their Security Policy, it's important to note that changes in legislation have brought mandatory data breach reporting to Canada. Administrative penalties surrounding these breaches can be assessed upwards of $100,000 per record.

My best advice is to build the Policy that bests presents the required behaviors for 'users and administrators' levels of information security to achieve the desired protection, security and availability objectives needed to secure your business data. Due to the changing methods of cyber-attacks the Security Policy needs to be updated regularly and can be considered a 'living document.

The scope of such a Policy encompasses computer information and information systems. This includes information that is stored on computer tapes, disks, and resident memory as well as information being transmitted electronically. The policy must apply to all business functions within an organization and including any subsidiaries.

Everyone in a business such as employees, consultants and its partners, vendors and contractors are required to safeguard the information assets your business possesses and even extends to its customers, shareholders and other third parties. They must maintain privacy consistent with legislation and the business operating policies and comply with vendor contracts, copyrights and patents. In addition, all information resident within a business or in custody of a person by reason of employment by the business, is the property of the organization and must be treated as privileged information to be used solely for duly authorized purposes. A Policy will not be successful in isolation; it needs the buy-in of all organizational executives, all the way down to the individual employee level throughout the company. It's about creating a culture that takes security into account as part of each person's regular job. The most brilliant Computer Information Security Group will still fail if they can't get buy-in from IT and other parts of the organization.

A good defense resides side by side with the Security Policy and both are your 'security tools'. Tools that are to be used or installed within your IT operating environments. For example Firewalls and Passwords to ensure secure environments. We also have anti-virus programs, anti-rootkit tools, malware detection, penetration testing and sniffing tools to proactively look for 'point of potential failure' within your IT operating environments.

Computer Information Security Policy - Roles and Responsibilities:

Corporate Security Executive (CFO, CIO, Internal Audit)

A Corporate Security Executive should be appointed and is responsible for directing the development, dissemination and periodic revisions of all supporting documents used for security purposes (eg. guidelines, procedures, bulletins). Whereas overall corporate security is directed by the Chief Financial Officer and Internal Audit, computer information security initiatives are directed by the Chief Information Officer.

Computer Information Security Group

The role of the Computer Information Security Group is to manage the implementation of the recommendations made by the Corporate Security Executive. This includes the administration of the Computer Security Awareness program and Business Resumption Plans for critical business processes.

In addition, this group will prepare security incident reports for presentation to the Corporate Security Executive for discussion and resolution planning. In terms of the executive, a well-structured organization would have separation of duties, e.g. Information Security Group would not report into the same chain of command as the people running the systems. This means that the Information Security Group should never report up to a CIO. It could however report up to an organizations' internal audit.

Information Owner

Each computer information system must have a defined owner. The individual(s) shall be designated to exercise management responsibility for granting overall access and disposition of each information resource. The owner is responsible for establishing the value or importance of information assets and classifying the information as per the organizations Information Protection Guidelines. This is another document that all business should have. All employees, consultants and contractors must thereafter abide by the proper handling, storage and disposal of sensitive information as per guidelines.

Exemption to a Computer Information Security

Exemptions to a Computer Information Security Policy may be granted where the guidelines and procedures recommended by the Computer Information Security Group cannot be applied for technical reasons or cannot be cost justified. Exemptions must be documented by the Information Owner and reviewed by the Corporate Security Executive for approval (*risk acknowledgement and 'assume' risk ownership*)

Want to learn more? The Government of Canada and Public Safety Canada have a useful document called **Get Cyber Safe - Guide for Small and Medium Businesses**. It can be found by clicking the link at: www.publicsafety.gc.ca/cyber This guide is designed to help Canadians who own or manage a small or medium business understand the cyber security risks they face, and provide them with practical advice on how to better protect their business and employees from cyber crime.

You can't predict a cybercrime event to your business, however proactively you can prepare to mitigate or eliminate the risk of one. ■