ITL INSURANCE THOUGHT LEADERSHIP

May 2, 2016

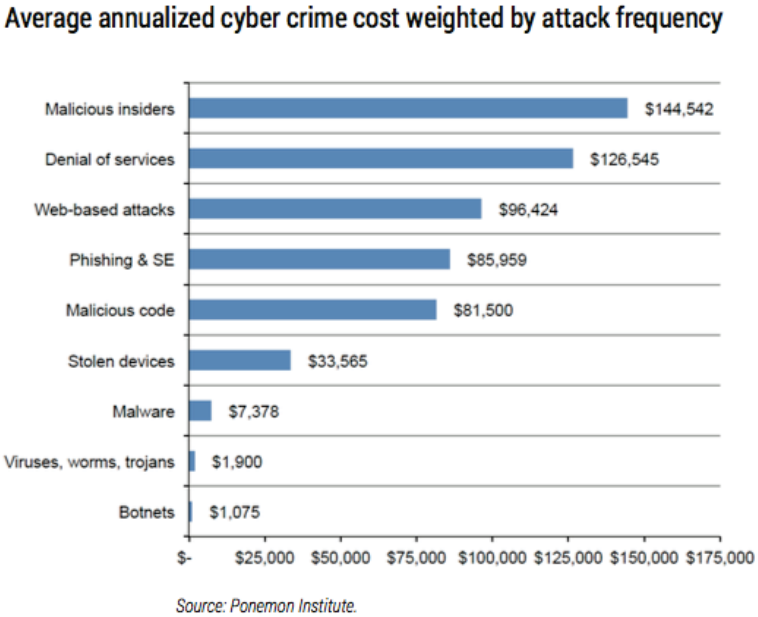
Best Practices in Cyber Security

Summary:

How can technology solutions be used to disarm hackers and prevent cyber losses, avoiding possibly significant claims?

By: *Brian Harrigan, Gary Miliefsky*

Cyber crime is the fastest-growing segment of the global criminal economy, now including state-sponsored hacking from the likes of North Korea, China and Russia. According to a 2015 FBI report, cyber crime has now overtaken illegal drug activity, moving into first place. As a result, the cyber liability insurance market is surging. Premiums are expected to top $5 billion by 2018. More than 60 companies currently offer cyber liability coverage on a standalone basis. Much of the underwriting for cyber risks includes the company-specific details and security breach data available in the public domain through websites such as According to Privacy Rights, nearly one billion records have been stolen from organizations of all sizes that are all running anti-virus software and firewalls. Unfortunately, anti-virus software misses as much as 30% of malware. Firewalls are perimeter traffic cops with no intranet security capabilities.



How does a savvy cyber insurance or reinsurance underwriter determine when breach-prevention measures have been taken by a given risk? How can today?s technology solutions be used to disarm the

hackers and prevent cyber losses, reducing the potential for a significant claim? Today, like never before, we face the frequent barrage of spear phishing attacks, new forms of very creative and nasty malware such as remote access Trojans (RATs), ransomware, zero-day malware (that means your antivirus doesn?t yet have a signature for the malware), not to mention the risks of malicious insiders, infected laptops coming and going behind our firewalls. In addition, many small and medium-sized businesses (SMBs) face increased scrutiny by government regulators. Cyber crime is growing at a tremendous rate ? it?s become an organized, big business opportunity for criminals, projected to grow to $600 billion this year, larger than any other form of crime, according to the World Bank. Cyber liability underwriters will want to appreciate what a network security, cyber risk management-focused, underwriting prospect looks like relative to the broader market.

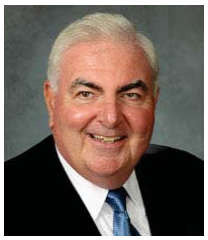
All cyber liability enterprise policyholders are not equal when measuring breach prevention methods and techniques that may be deployed with an eye toward mitigating significant future losses. You might ask ? why would my smaller business be a target ? we?re not Bank of America ? we?re not Home Depot or TJMAXX or Anthem? Yes, they all are big targets for big hackers, but cyber criminals don?t discriminate. In fact, they find SMBs easier targets because, traditionally, your level of defenses against cyber crime might not be as advanced as those at Bank of America ? which has a $400 million annual information security budget. To the cyber criminals in in the dark corners of the Internet, you?re called a "soft" target ? they feel you are easier to exploit. One piece of ransomware and you might be out of business. Some of the latest ransomware exploits will not only encrypt your laptop or desktop, but they also look for file servers and do the same, automatically. Then, you won?t have any access to your own files ? or, even worse, customer records ? until you pay the ransom. The FBI even recommends you pay the extortion fee. We find this all wrong. It?s completely backward. We cannot let ourselves be victims. It?s

time to get more active and be one step ahead of the next attack ? you are a target but you don?t have to be a victim. It all starts with best practices. For example, if you did frequent daily backups and tested these backups, then, when you?ve been victimized by ransomware, instead of paying the extortion fee, why not wipe the infected computer, re-image it then restore the latest backup? When asked, most SMBs say "I don?t do frequent, daily, backups? or ?I haven?t figured out how to wipe and re-image all of our systems in the event they get infected.? So, it?s that simple, one best practice ? Backup and Restore -- would save you thousands of dollars in extortion fees. You could thumb your nose at the cyber criminals instead of giving them some of your hard-earned revenue. Cyber liability policy terms and conditions should reflect more favorably on ?Breach Prevention?-focused organizations. Best practices are things you do - steps you take - actions and plans, risk management and claims mitigation techniques. Within those plans, we are certain you will include which security countermeasures to budget for this year. **Seven Best Practices to Reduce Risk** Although we thought about going into details about recent security concepts, such as next-generation endpoint security or network access control, it seems more appropriate to focus on the best practices instead of the best security tools you might consider deploying. For example, we consider encryption a best practice and not a product or tool. We are sure you'll find many commercial and freely available tools out there. You can always evaluate those tools that you find most suited for your own best-practice model. So let?s consider the following as MUST-DO best practices in cyber security to defend your SMB against the risk of a breach: 1) Roll out corporate security policies and make sure all your employees understand them. 2) Train employees and retrain employees in key areas ? acceptable use, password polices, defenses against social engineering and phishing attacks. 3) Encrypt all records and confidential data so that it?s more secure from prying eyes. 4) Perform frequent backups (continuous backups are even better than daily backups) and have a re-image process on hand at all times. 5) Test your system re-imaging and latest backups by restoring a system to make sure the backup-restore process works. 6) Better screen employees to reduce the risk of a malicious insider. 7) Defend your network behind your firewall using network access control (NAC) ? and make sure you can block rogue access (for example, the cleaning company plugging in a laptop at midnight) and manage the bring your own device (BYOD) dilemma.

More Than 95% of Breaches Happen Behind Firewalls ? It?s Usually an Employee Mistake How many times have you heard of a trusted insider falling for a phishing scam or taking a phone call from someone sounding important who needed "inside" information? It's happening too frequently to be ignored. Some employees love browsing Web sites they should not or gambling online or

chatting using instant messenger tools. You need to educate them about acceptable usage of corporate resources. They also usually don't know much about password policies or why they shouldn't open the attachment that says "you've won a million - click here and retire now." It's time to start training them. Invite employees to a quarterly "lunch and learn" training session. Give them bite-sized nuggets of best practice information. For example, teach them about the do's and don't's of instant messaging. If you are logging e-mail for legal purposes, which in some cases is required by law (SEC requirements for financial trading firms), let them know that you are doing it and why you are doing it. Give them some real-world examples about what they should do in case of an emergency. Teach them why you've implemented a frequent-password change policy and why their password should not be on a sticky note under their keyboard. Let these sessions get interactive with lots of Q&A. Give an award once per year to the best security compliant employee who has shown initiative with your security policies. If you can keep them interested, they will take some of the knowledge you are imparting into their daily routines. That's the real goal. **Are My Best Practices Working? Time for Self-Assessment Before an Audit** Perform your own security self-assessment against these best practices recommendations I?ve listed above. Find all of the holes in your information security environment so that you can, document them and begin a workflow process and plan to harden your network. Network security is a process, not a product, so to do it right, you need to frequently self-assess against the best guidelines you can find. Boards of directors, CEOs, CFOs and CIOs are under extreme compliance pressures today. Not only are they charged with increasing employee productivity and protecting their networks against data theft, but they are also being asked to document every aspect of IT compliance. We recommend, whether or not an outside firm is performing IT compliance audits, that you begin performing measurable compliance self-assessments. You'll need to review those regulations that affect your organization. In the U.S., these range from GLBA for banks to HIPAA for healthcare and insurance providers to PCI for e-tail/retail to CFR-21-FDA-11 for pharma to SOX-404 for public companies. Some states have their own regulations. In California, for example, if there has been a breach in confidentiality due to a successful hacker attack, companies are required by law to publish this information on their Web sites. The California Security Breach Information Act (SB-1386) requires the company to notify customers if personal information maintained in computerized data files has been compromised by unauthorized access. California consumers must be notified when their name is illegitimately obtained from a server or database with other personal information such as their Social Security number, driver's license number, account number, credit or debit card number, or security code or password for accessing their financial account. If you are a federal government agency, you need to comply with Executive Order 13231, to ensure protection of information systems for critical infrastructure, including emergency preparedness communications and the physical assets that support such systems. Also, if you are a non-profit organization, you are not exempt from the reporting requirements of regulations in your industry (banking, healthcare, etc.). Please make sure to seek legal counsel if you are not sure of which regulations you'll need to address. The easiest thing you can do to prove you are in compliance is to document your steps of protecting data. **Document Your Best Practices** Documentation showing that you?ve implemented best practices for risk reduction and against cyber crime will come in handy if you ever have a breach and need to defend yourself to enforce your cyber insurance policy or to keep the government regulators off your back. This kind of documentation is also good in the event

someone sues your organization. You should be able to prove that you have in place all the best policies and practices as well as the right tools and INFOSEC countermeasures for maintaining confidentiality, availability and integrity of corporate data. By frequently assessing your compliance posture, you'll be ready to prove you "didn't leave the keys to the corporate assets in the open." If your network is ever hijacked and data is stolen, you'll have done your very best to protect against this event and it will be less of a catastrophe for your organization. Do you have a cold, warm or hot backup site in case of a critical emergency? If not, you should start planning one. If you can't afford one, could you create a "virtual" office telecommuting situation where your organization could continue to operate virtually until you've resolved your emergency situation? Knowing we are under constant attack and risk, now is the best time to begin implementing these seven best practices for network security. Hackers, malicious insiders and cyber-criminals have had their field day this year, and it?s only going to get worse - hijacking our SMB networks and placing most organizations at risk of being out of compliance, tarnishing our brands, reducing our productivity and employee morale -- placing most of us in the passenger seat on a runaway Internet. By taking a more active approach, setting measurable goals and documenting your progress along the way, you might find yourself in the drivers? seat of cyber security.



Brian Harrigan

Brian.Harrigan@gboiq.com

Brian Harrigan, a 39-year veteran of the insurance and employee benefits segment, is president and CEO of GBO/Insur IQ. GBO focuses on the digital distribution and automated, real-time underwriting and policy administration of insurance products across the life, A&H and P&C spectrum.

Gary Miliefsky

garym@snoopwall.com

Gary Miliefsky is a consumer advocate who has been featured on NBC?s Today, FOX News, CNBC and elsewhere for his expertise in cyber security. He is founder of SnoopWall, a cutting edge counter-intelligence technology company offering free software to secure personal data on cell-phones and tablets.