Battling Security Fatigue – Working Towards Usable Security

Security the Unfortunate Equalizer…

J.P. Morgan Chase spends about half billion dollars on cybersecurity. Why?

* Ability of the Firm to maintain the security of its financial, accounting, technology, data processing and other operating systems and facilities.
* Ability of the Firm to effectively defend itself against cyberattacks and other attempts by unauthorized parties to access the Firm's information or disrupt its systems.

How much is your Financial Institution (FI) spending on cyber-security?

Sure, with more locations, computers, employees and vendors there is more to manage from a security perspective. However, just putting in the basic required Tools, Policies, Plans and Processes (TPPP) can be unaffordable for smaller FIs. However, FIs must invest in cyber-security or they will have a price to pay (either with criminals or regulators).

* InfoSecurity Magazine - Financial services firms are hit by security incidents 300 times more frequently than businesses in other industries.
* Deloitte Banking Outlook - The financial services sector faces the greatest economic risk related to cybersecurity.

Criminal bad actors attack smaller FIs because they know they are not investing at the same level as organizations such as J.P. Morgan, Bank of America, Citibank, and Wells Fargo who are collectively spending $1.5 billion to battle cybercrime.

One saving grace is that most criminals are not the cyber geniuses you see on television creating "zero day" exploits—most common cyber criminals simply use old exploits that they can download, update and easily deploy. However, the bad news is that a common bad actor is smart enough to find an organization's vulnerabilities on https://shodan.io, find default passwords on sites like http://defaultpassword.com, download ransomware exploits from CyrptoLocker that have been developed by groups like FAKBEN, and use tools like http://execrypt.com to get around anti-virus software—it's not hard, in fact it's quite trivial. Plus most FIs with a firewall and anti-virus software will not detect they are being ripped off until it's too late…

So where does money need to be invested? The answer is in the TPPP but it doesn't need to be expensive if you stay on top of the "Managed Detection & Response" (MDR) industry.

Security products and services can be incredibly expensive and spending money on technology that does not increase productivity can be hard to justify. FIs need a layered approach to security with a minimum of 3 layers – Firewall and Endpoint protection as the first two and the third being Continuous Monitoring of the network for any bad actor that makes it through the protection (usually let in by a user by clicking on something, sending something or running something that creates a vulnerability). Another tool that is essential is a 1st & 3rd party cyber liability insurance.

… But tools and services are only a small part of the solution. A less expensive, yet more important, part of the solution are good Policies, Plans and Processes that are well articulated, understood and practiced (this is where good leadership and management comes into place).

Your FI needs to have in place Policies such as:

* Acceptable Use Policy (more info)
* Remote access policy (more info)
* Employee termination and out-processing policy
* Password policy (more info)
* Encryption policy (Great example)… More info on encryption.
* Bring your own device (BYOD) policy (Great example).
* Vendor Management Policies – if they are on your network or have your data they need to be as secure as you are... so put it in their contract!

More example policies can be found here. … and most important, you need a training policy that ensures that your staff understands both what are in these policies and how to protect themselves from bad actors.

In regards to Plans, do you have (and update) a disaster recovery/business resumption plan? For Processes -- Do you test your data backup/restore processes? Are you keeping the firmware up-to-date on all your networking equipment and servers/computers? Are you keeping all your systems (operating systems, firewalls, software solutions, Flash, Java etc.) up to date with the latest security patches?

As you can see, great Policies, Plans and Processes can be both inexpensive to create and manage but have a very big impact on limiting your exposure to being compromised.

You can also minimize your investment in tools and services if you keep up with advancements in the cyber technology industry. The MDR services that are being offered in the last couple years drastically reduces that cost associated with continuous monitoring leveraging both automation as well as third party analysts. Such a solution is https://netwatcher.com that can be as low as $299 a month for basic services. With an MDR solution like NetWatcher you can have an enterprise continuous security monitoring at an affordable price and it will be there to catch you if something gets by your other TPPPs!

Scott B. Suhy
CEO

NetWatcher

Contact Info

www.netwatcher.com

Scott B. Suhy has successfully built businesses for large, mid-size and start-up companies over the past 25 years. Scott has a great balance of deep technical skills, broad leadership, and business experience. Prior to NetWatcher, Scott co-founded PointAbout (a mobile applications company sold to 3Pillar Global), grew GreenLine Systems (a data analytics company sold to AT Solutions) and was a General Manager at Microsoft for over 15 years. Scott has a BS in Engineering from the University of Pittsburgh.

NetWatcher is the first enterprise-class cyber security solution designed for mid-sized businesses, keeping an eye on their networks and looking for anomalous behavior 24x7. PCI DSS, SOX, ISO, GLBA, and other compliance programs require log storage, management and monitoring. NetWatcher can help you protect your data and prove compliance. NetWatcher is priced very competitively on a per monitored network model, not by log volume. This means you have one low monthly fixed price with no large up front investment.