Breaking The Cyber-Security Console

by Steve Brown

President Obama has unveiled a cybersecurity national plan to update aging government networks and boost security awareness. The plan is the White House's response to the last epidemic of data breaches, in both the public and private sectors. The President wants to put aside $3B to modernize the patchwork of computer systems used in government agencies. "It is no secret that too often government IT is like an Atari game in an Xbox world" declared the President.

After all, hackers have a lot of fun exploiting the holes in public networks. Last year data from 20mm federal employees and contractors leaked from the Office of Personnel Management. The private sector is also exposed. Newspapers and magazines are full of horror stories about people who are victims of massive cyber attacks.

Financial institutions are on the alert too and are certainly not immune to hackers' malevolence. To strengthen your practices, consider going back to the basics. Eliminate and take offline any and all data that is not necessary to keep on servers. If it isn't on the server it can't be stolen no matter how sophisticated the foe you are facing.

Start with personally identifiable financial information. This is defined by the FFIEC as any information a financial institution obtains about a consumer in conjunction with providing a financial product or service. The FDIC defines this further as any information about an individual which can be used to distinguish or trace that individual's identity, such as their full name, home address, email address (non-work), telephone numbers (non-work), Social Security Number (SSN), driver's license/state identification number, employee identification number, date and place of birth, mother's maiden name, photograph, biometric records (e.g., fingerprint, voice print), etc. This also includes, but is not limited to, education, financial information (e.g., account number, access or security code, password, personal identification number), medical information, investigation report or database, criminal or employment history or information, or any other personal information which is linked or linkable to an individual.

Then, compare what you have to what is publicly available. This type of information is defined as information that a financial institution has a reasonable basis to believe is lawfully and publicly available from sources such as: public records, widely distributed media, and government-required disclosures. This comparison should result in areas you should focus on and move immediately to remove where possible and heavily encrypt where not possible.

There are lots of ways the bad guys can get into your systems and many in the IT world would say they are probably already there just watching and waiting to strike. That's why we suggest moving to a simpler approach of, if you don't need it to be on your systems, delete it completely. Then, if an evil doer gets in, they will only find a handful of sensitive data vs. a bucket full.

In the meantime, continue to train your staff, add security layer upon security layer to better protect you, and monitor activity on all computers in as real time an environment as you can.

Finally, be sure to target what may be your weakest link - your customers. Remind and train them to protect themselves and in turn protect your bank. Good luck and keep playing this game with the best tools you can find.

BANK NEWS

Social Media

A survey of small businesses by Wasp Barcode Technologies finds the following ways owners say they use social media to try and grow their business: promote a specific product or service (45%); share information about promotions, sales and discounts (38%); gain likes and fans (38%); solicit or respond to customer feedback (34%); provide videos highlighting my products or services (29%); recognition from my employees (28%); share a company blog or blog post (28%); establishing my personal expertise (23%); and provide training videos for customers (18%).

Model Limits

The Basel Committee is proposing limiting the ability for banks to use internal models to calculate certain types of credit risk and instead would have to use a standardized method (would require minimum levels of capital to be set aside for certain loan types). Basel is taking the action in an effort to tighten up moves by banks to potentially stretch limits when calculating risks to other banks, corporations, etc.

Fiduciary Standard

The Wall Street Journal reports the White House is seeking to finish its fiduciary standard rule on brokers and others who advise investors in IRA and 401(k) retirement accounts by early Apr. Meanwhile, the Labor Department is seeking to adopt the rule as soon as Apr 4.

Comfortable Retirement

Research by the EBRI on retirement finds workers who say they are very confident about having enough money for a comfortable retirement reached 21% this year vs. the record low of 13% from 2009 to 2013.

Planning Problems

A survey of family businesses by Kreischer Miller finds the following reasons these businesses do not have a succession plan in place: still figuring it out (21%), age and ability (15%), plan to sell (12%), not sure (12%), agreement (12%), other (12%), time (8%) and resources (8%).

CRO Reporting

A survey on risk practices by Bank Director finds the chief risk officer reports to the following among others: CEO (72%), risk committee (34%), audit committee (24%), board (20%) and other officer (20%).