Perspectives on Cybersecurity

October 11, 2019
The **dark web** refers to encrypted online content that is not indexed by conventional search engines. Also known as the "darknet," the **dark web** is a component of the **deep web** that describes the wider breadth of content that does not appear through regular internet browsing activities.  

Jun 25, 2019
Our Panel

2 bankers, and auditor and a pair of insurance agents walked into the DARK WEB…….

- Maureen Hegarty and Darcy Lawn  Iberia Bank
- Mary Brown, CPA;  PDR CPA’s
- Steve Follos and Paul Stephens; Church Insurance
Prevent
Banking

Catch/Identify
Auditing / Financial Statements

Manage
Insurance
Prevent Banking
In 2018 the Association for Financial Professionals published its 14th annual survey about commercial payments fraud. Among the results . . .

- 78% of organizations experienced attempted or actual payments fraud in 2017. (Up from 60% in 2013)
- The payment methods most often targeted for fraud:
  - Checks (74% of incidents)
  - Wire Transfers (48%, up from 14% in 2014)
  - Commercial Credit Cards (30%)
  - ACH Debits (28%)
  - ACH Credits (13%)
How Does Check Fraud Occur?

If I’m a check issuer for the organization I can write small checks that will not call attention to themselves in the check register...

...And then alter the payee line to make it payable to me.
How Does Check Fraud Occur?

If I receive a check from you, I can wash the amount . . .

---

ABC Company  
1234 Fifth Street  
Tampa, Florida 34695

Date: June 11, 2016

Pay to the Order of  
Ace Plumbing Company  
$ 10000000.00

One gazillion and 00/100

Main Street Bank  
Tampa, Florida 34689

Memo

. . . and remake the check for a higher amount.
How Does Check Fraud Occur?

Let's just wash the whole thing...

ABC Company
1234 Fifth Street
Tampa, Florida 34695

Pay to the Order of ____________________________ ________________ $ ____________

Main Street Bank
Tampa, Florida 34685

Stamp it VOID...

...And send it off to a check printer to "re-order" a whole box of blank checks.
More Results from the AFP Survey

Business Email Compromise is quickly growing as a method for committing financial fraud, amounting to $5.3 Billion over three years.*

- 77% of survey respondents said they have experienced Business Email Compromise.
- In this scheme:
  - An associate with payments capability will receive an email that appears to be from an executive of the company.
  - The message will describe an urgent need for a payment to be sent to support an important transaction, usually in the form of a wire transfer but sometimes by check or commercial credit card.
  - The message will normally present a reason why the executive cannot be contacted for confirmation. (“I’m about to get on a plane. I’ll call you when I land.”)
  - The message – and the wire – are fraudulent.

*Source: The Federal Bureau of Investigation
Teach Your Team About the Risk of Emails

Don’t click this link!
Not from your bank
Not from the IRS
Not from the FDIC
Not from your Mom

This is how malware gets loaded to your computer.

Here at the West River Bank, we are very concerned about the security of your account information. For that reason, we have created a set of “Best Practices” our customers should follow whenever they interact with the bank online.

Please click on the link below to review this important security information.


Shirley Eugest
VP, Manager of Customer Security
West River Bank
888.555.4321
Teach Your Team About the Risk of Emails

Would it help if you were to contact the sender to validate the message is genuine?

Here at the West River Bank, we are very concerned about the security of your account information. For that reason, we have created a set of ‘Best Practices’ our customers should follow whenever you interact with the bank online.

Please click on the link below to review this important security information.


Shirley Eugest  
VP, Manager of Customer Security  
West River Bank  
888.555.4321

Good idea! But don’t use the contact info in the message. If this is a fraudulent message, the crook will gladly confirm its legitimacy.
The messages can look highly official. Here is a real world example . . .

From: alert@federalreserve.gov [mailto:alert@federalreserve.gov]
Sent: Monday, March 14, 2016 8:35 AM
To: Kxxxxxx  Bxxxxxx
Subject: Wire transfer was canceled

The Domestic Wire fund transfer, recently initiated from your checking account, was not processed by the Federal Reserve Wire Network. Please click here to view report

This service is provided to you by the Federal Reserve Board. Visit us on the web at http://www.federalreserve.gov
Even “internal” emails can contain risk.

From: Crook, Ima [mailto:icrook@ibereabank.com]  
Sent: Thursday, March 17, 2011 3:00 PM  
To: Associate, Susie  
Subject: Suspicious Activity Alert, Please Read Immediately

Susie, I am with the security team, and we have noticed a large amount of suspicious activity originating from your machine. The log files indicate that a spyware program is installed on your machine which has captured your domain password. This password needs to be changed immediately. Please log in [here](mailto:icrook@ibereabank.com) and change your password immediately to stop the effects of the virus.

Ima Crook  
Information Security Architect
Preventing and Detecting Email and Online Fraud.

The Internet has transformed the way we do business, including marketing, sales, and engaging in banking services. Unfortunately, increasing online usage has been followed by increasing online criminal activity. Protecting against email and online fraud requires adherence to sound preventative measures and practices — a number of which are included below for your consideration.

What you should know about business email fraud and online fraud:

Hackers perpetrate scams in many ways. A common way is to send fraudulent email appearing to be from a known source (an executive of your company or a client, for example) requesting bank transactions or other financial information. Hackers can also fabricate or steal an email address and use it to invite you to click on a link to a bogus website. If you follow the email instructions from a fraudster or provide confidential information, such as your user ID, password, account number, or tax ID number, then online fraud can take place, potentially putting you and your company at risk.

By proactively enhancing your company’s security, you can reduce the risk of email fraud and online fraud and minimize threats.

Safeguard your company’s online access and password:

- Create passwords that are not easily guessed. Avoid using personal information, such as your last name or birthday.
- Use different user IDs and passwords for multiple websites.
- Don’t record or save passwords, IDs, or other sensitive information on your computer.
- Don’t share your passwords or other login credentials with anyone.
- Don’t share company user IDs. Each user must have a unique user ID and password.
- Remind users to change their passwords frequently.
- Log out or lock your computer when you are away from your workstation.
- Avoid using automatic login features that save usernames and passwords for online banking.
- Never access bank, brokerage or other financial services information at Internet cafes, public libraries, etc. Unauthorized software may have been installed to tap account numbers and sign on information leaving you vulnerable to possible fraud.

Maintain internal controls and policies:

Maintain appropriate internal controls, including segregation of duties, and periodically review them. For example, require one user to set up or initiate payments and another to approve the payments. Make sure to delete user profiles that no longer need access.

- When approving transactions, carefully review all details, paying close attention to the beneficiary routing number and account number.
- Set up customized account alerts, like balance minimums, through online banking, so you know when certain account activity takes place.
- If your company processes ACH batches, approve them individually.
- If your company initiates ACH and wire transfer payments, consider using dual control (originator and authorizer).
- Verify payment or change requests with the vendor. You could receive a fraudulent email disguised to be from a known vendor. When a payment is made, the funds are sent to the fraudster instead of the intended vendor.
- Review and reconcile banking transactions daily.
- Perform periodic risk assessments of the banking products/services your company uses, including regular reviews of user access levels, dollar limits and activity.
Cybersecurity

- Estimated 1,300 data breaches affecting 174 million records reported in 2017 (30% increase from 2016)
- Approximately 63% of NFP’s reported at least one breach in the last year
- Healthcare & education institutions have incurred the most breaches to date for NFPs (Privacy Rights Clearinghouse)
- Most reported breaches are due to hacking, email phishing, or malware – especially ransomware
- Mobile ransomware infections have risen over 250% in Q1 of 2017

Source: AICPA Not-for-Profit Entities: 2018 Audit and Accounting Issues
Cybersecurity - Continued

- Breaches are often a result of improperly secured systems and lack of user education
- It is important that IT systems are current and include rigorous protections to deter and detect attacks, such as:
  - Network infrastructure design
  - Encryption of sensitive data
  - System access limitations
  - Anti-malware and data leakage strategy
  - Backup and restoration processes

Source: AICPA Not-for-Profit Entities: 2018 Audit and Accounting Issues
Responsibilities of Those Charged with Governance:

- Oversee the financial reporting process

- Set a positive tone at the top and challenging management’s activities in the financial arena

- Discuss significant accounting and internal control matters with management

- Inform the auditor about fraud or suspected fraud, including its views about fraud risks

- Inform the auditor about other matters that are relevant to the audit
Data Analytics:

**Benford's law**, also called the **first-digit law**, states that in lists of numbers from many (but not all) real-life sources of **data**, the leading digit is distributed in a specific, non-uniform way. According to this law, the first digit is 1 almost one **third** of the time, and larger digits occur as the leading digit with lower and lower frequency, to the point where 9 as a first digit occurs less than one time in twenty. This distribution of first digits arises whenever a set of values has **logarithms** that are **distributed uniformly**, as is approximately the case with many measurements of real-world values. This counter-intuitive result has been found to apply to a wide variety of data sets, including electricity bills, street addresses, stock prices, population numbers, death rates, lengths of rivers, **physical** and **mathematical constants**, and processes described by **power laws** (which are very common in nature). The result holds regardless of the **base** in which the numbers are expressed (except for trivial bases), although the exact proportions change. It is named after physicist **Frank Benford**, who stated it in 1938, although it had been previously stated by **Simon Newcomb** in 1881.
Example of a bad graph – the number 3 is well out of expected limit:
Diocese Debits:
Diocese Credits:
Manage

Insurance
Some statistics from CIAC:

- Small business/organization breaches grew by 44% over the past two years – the average cost more than doubled during this time.
- Hacking and malware virus’ caused 45% of all breaches – followed next by human error.
- The median cost of a small breach is $32,500.
- Crisis Services (Forensics, Legal, etc.) are 78% of the total breach claims cost.
- In 2015, a sizeable 3.4% of the 40,000 daily cyber attacks were aimed at religious organizations. That has only increased since, but I can’t get a certain figure yet.
- The insurance industry projected that for 2018 the industry that might expect to become a threat of cyber attacks was Religious Organizations.
New and Emerging Risk — Cyber Liability

Provides insurance coverage for claims made against the church that typically arise from failure to protect sensitive information, including subsequent actions by a regulator.

Breach Costs coverage provides insurance for the typical costs that the church could incur arising from the failure to protect personal information. Coverage applies to a breach first discovered during the policy period.

Multimedia Protection provides insurance coverage for claims made against the church that arise from the content of your website, social media and other promotional material.

Hacker Damage coverage provides insurance for the costs to repair or replace your website, intranet, network, computer system, programs, or data following a hacking event.

Cyber Business Interruption provides insurance coverage for your losses resulting from a hacker impairing the availability of your website, intranet, network, computer system, programs or data.

Cyber Extortion provides insurance coverage for the costs of expert assistance and the payment of a ransom in the event that a hacker threatens to damage the church website, intranet, network, computer system, any programs used or data.
Cyber Liability

- Provides both first and third party insurance for covered cyber losses.

- First-party coverage insures for losses to the policyholder’s own data or lost income or for other harm to the policyholder’s business resulting from a data breach or cyber-attack.

- Third-party coverage insures for the liability of the policyholder to third parties — including clients and governmental entities — arising from a data breach or cyber-attack.
# Cyber Liability

<table>
<thead>
<tr>
<th>Liability Coverage</th>
<th>Liability Limit</th>
<th>Deductible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multimedia Liability</td>
<td>$250,000</td>
<td>$1,000 each Claim</td>
</tr>
<tr>
<td>Security &amp; Privacy Liability</td>
<td>$250,000</td>
<td>$1,000 each Claim</td>
</tr>
<tr>
<td>Privacy Regulatory Defense</td>
<td>$250,000</td>
<td>$1,000 each Claim</td>
</tr>
<tr>
<td>PCI DSS Liability</td>
<td>$250,000</td>
<td>$1,000 each Claim</td>
</tr>
<tr>
<td><strong>Non-Liability Coverage</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Breach Response Costs</td>
<td>$250,000</td>
<td>$1,000 each Claim</td>
</tr>
<tr>
<td>Voluntary Notification Costs Sublimit</td>
<td>$250,000</td>
<td>$1,000 each Claim</td>
</tr>
<tr>
<td>Proactive Privacy Breach Response Costs Sublimit</td>
<td>$250,000</td>
<td>$1,000 each Claim</td>
</tr>
<tr>
<td>BrandGuard®</td>
<td>$250,000</td>
<td>2-week waiting period</td>
</tr>
<tr>
<td>Network Asset Protection</td>
<td>$250,000</td>
<td>$1,000 each Claim</td>
</tr>
<tr>
<td>Cyber Extortion</td>
<td>$250,000</td>
<td>$1,000 each Claim</td>
</tr>
<tr>
<td>Cyber Crime</td>
<td>$25,000</td>
<td>$1,000 each Claim</td>
</tr>
</tbody>
</table>
Example of a cyber extortion claim

- We had an extortion claim at a cathedral within a week of putting the coverage in place. They were stating that they had social security numbers and other personal information such as credit and debit card numbers and wanted money or they would release and use the information. The group we use negotiates and even more importantly works to make sure it does not happen again.
Ransomware—Kidnapping Your Company Data

What is Ransomware?
Ransomware is a type of malware (malicious software) that 'kidnaps' your business data and holds it hostage until you pay a ransom. Ransomware holds your data hostage by encrypting it and preventing access to it. If the ransom is paid, the decryption key is sent to you to decrypt and ideally recover your data. If the ransom is not paid, your data remains encrypted and unusable.

Ransomware in the News
In 2017, ransomware attacks spiked with several attacks making the mainstream news. For example, WannaCry and NotPetya were two ransomware variants that made major headlines last year. WannaCry alone affected more than 300,000 organizations worldwide. Ransomware attacks are growing and employees play a big part in protecting an organization against ransomware.

How Does Ransomware Get on Your System?
Ransomware typically enters your network through outdated software, or, more commonly, when an employee responds to a phishing email by clicking on a link or opening an e-mail attachment containing malware.

Best Practices
Here are some ways you can help to defend against ransomware attacks.

- Recognize phishing emails. Don’t open any attachments or click on any links in suspicious emails. Forward them to your IT department for verification. If you don’t know how to recognize a phishing email – ask your IT department for help.
- If infected, IMMEDIATELY disconnect your computer from all networks and call your IT department.
- Always regularly back up business critical data and store backups disconnected from your network. You don’t need to pay ransom if you have good backups!
- Keep all software on your computer up-to-date.
CYBERSECURITY TRAINING BULLETIN

THE IMPORTANCE OF HAVING A “CLEAN DESK”

What is a “clean desk”?

A “clean desk” is a workstation that does not expose any sensitive or confidential information to those in proximity and that has the information secured in a locked area and out of sight when not being used.

Why is a “clean desk” important?

Having a clean desk is important because it significantly reduces the risk of information theft, fraud, or a data breach caused by sensitive information being visible in plain view.

Best Practices

What can I do to keep a “clean desk”?

Here are several ways you can have a clean desk.

- Secure all sensitive/confidential information in hardcopy or electronic form in your work area at the end of the day and when you are expected to be gone for an extended period.
- Lock or shut down your computer when the workspace is unoccupied or at the end of the day.
- Remove any sensitive/confidential information from your desk and lock in a drawer when the desk is unoccupied and at the end of the work day.
- Don’t post passwords on or under a computer or in any accessible location.
- Immediately remove printouts containing sensitive/confidential information from the printer.
- Shred documents containing sensitive/confidential information in official shredder bins or place in locked confidential disposal bins.
- Erase whiteboards containing sensitive/confidential information.
- Secure storage devices such as CDROM, DVD or USB drives in a locked drawer.
THE IMPORTANCE OF MOBILE DEVICE (LAPTOP) SECURITY

Lost and stolen laptops and mobile devices directly affect an organization’s bottom line.

The cost of a lost or stolen device is far greater than just the price of the device. Other costs include the value of the data on the device, fines and penalties from regulators, the reputational harm of a potential data breach and more.

So - keeping your laptops and mobile devices secure is very important!

Use these tips to keep your laptops and mobile devices secure!

- Laptops should always be stored in secure areas.
- Never leave laptop bags unattended in airports or other public facilities, and always use the hotel safe to secure equipment when you’re not in the room.
- When traveling, keep laptops in the trunk and out of sight (if they must be left in the car).
- When flying, do not put laptops in your checked bags - secure your laptop in your carry-on bag.
- Don’t keep your laptop passwords with the laptop or its case.

What if my laptop is lost or stolen?

If any device you use for work (including your own devices like a smartphone or laptop) is lost or stolen, IMMEDIATELY contact your supervisor, IT department or other individual as specified in your organization’s mobile device management policy.

Cybersecurity is a team effort. Every employee counts, and participation is needed to maintain a good security posture.
Questions
from the Audience
Maureen Hegarty
Vice President
IBERIABANK | Treasury Management Sales Officer
201 North Franklin Street, Suite 100
Tampa, FL 33602
Office: (813) 603-4180 | Cell: (813) 417-3928
maureen.hegarty@iberiabank.com

Darcy Lawn
Vice President / Branch Manager
IBERIABANK
5310 State Road 64 East
Bradenton, FL 34208
Office: 941-487-3052 | Cell: 941-284-6945
darcy.lawn@iberiabank.com

Mary Brown, CPA
Shareholder
Mailing Address
4023 Tampa Road, Suite 2000 | Oldsmar, FL 34677
P 727.785.4447 | P 813.498.1294 | F 727.784.5491
Local Firm. National Level Resources.

Steven Follos, General Manager
Church Insurance Agency Corporation
For service call (800) 293-3525
Direct (802) 753-1355
YOU are the LIGHT of the WORLD

51st ANNUAL CONVENTION