Cyber *Insecurity*
What you Can do Now to Help Keep Your Organization Safe

John Ansbach, JD, CIPP-US
@johnansbach
jansbach@strozfriedberg.com

STROZ FRIEDBERG
an Aon company © 2017 Stroz Friedberg. All rights reserved.
“On December 22, 2017, Jason’s Deli was notified by payment processors that credit card security personnel had informed it that a large quantity of payment card information had appeared for sale on the “dark web,” and that [ ] at least a portion of the data may have come from various Jason’s Deli locations.”

“…criminals used [ ] malware to obtain payment card information off of the POS terminals beginning on June 8, 2017… approximately 2 million unique payment card numbers may have been impacted…”
A ransomware attack that began in Europe has now spread to targets in Japan and China. The WannaCry strain infected computers in more than 150 countries. Users were asked to pay a $300 payment to restore their files.

The WannaCry ransomware first surfaced over the weekend as reports of infections streamed in from around the globe. It was the stuff of a bodacious techno-thriller, and we watched it unfold in real time. But how did WannaCry come to be? How did it infect so many computers so quickly? And, perhaps most importantly, how will organizations and individuals cope with the fallout?

What is MS17-010, and what does it have to do with WannaCry?

When Microsoft needs to alert its customers to a security concern, it creates bulletins and posts them to the TechNet site. They’re given a label and assigned a severity rating. MS17-010 is a bulletin Microsoft posted in March. It disclosed the existence of a critical vulnerability in an older version of the SMB network protocol. That vulnerability was exploited by WannaCry to spread from computer to computer.
How John Podesta's Emails Were Hacked And How To Prevent It From Happening To You

Fancy Bear was responsible for the hacks on John Podesta, Colin Powell and the Democratic National Committee (DNC)…

Fancy Bear used a spear-phishing campaign to attack their victims.

The Podesta spear-phishing hack was instigated with an email that purported to come from Google informing him that someone had used his password to try to access his Google account. It included a link to a spoofed Google webpage that asked him to change his password because his current password had been stolen.
Podesta clicked the link and changed his password. Or so he thought. Instead, he gave his Google password to Fancy Bear and his emails began appearing on WikiLeaks in early October.

A screenshot of the phishing email received by Rinehart. (Image: The Smoking Gun)
"Podesta clicked the link and changed his password…Or so he thought…

Instead, he gave his Google password to Fancy Bear and his emails began appearing on WikiLeaks in early October."

As reported by Motherboard, the Russian hacking group Fancy Bear hacked John Podesta, who had also worked for Hillary Clinton's campaign at the time. They targeted Podesta and the Democratic National Committee (DNC) and used spear-phishing attacks to steal passwords and obtain access to their email accounts. The hackers then leaked Podesta’s emails on WikiLeaks.

**Phishing, spear phishing and the Podesta hack**

Phishing scams try to trick people into giving up information like passwords, or bank account and credit card numbers through emails that falsely claim to be from a “trusted” source. An early example of phishing is the notorious Nigerian bank scam in which an email promised to gift you with a lot of money if you would give up your banking information in order to help someone move money out of Nigeria. Phishing attacks are usually sent to large numbers of random email addresses.

Spear-phishing is a more sophisticated form of phishing that targets individuals using personally relevant information. The spear-phishing email purports to come from a friend, a company you do business with such as your bank, or an Internet friend whom you trust and know to be reliable.
A security breach in the Utah Food Bank's website may have resulted in the disclosure of more than 10,000 donors' personal information… In a letter that was sent to a donor on Tuesday [], Utah Food Bank officials said they recently discovered that an "unauthorized individual" may have gained access to donation information submitted through the organization's website…Names, addresses, emails, credit or debit card numbers, security codes and expiration dates may have been exposed during that time period, the letter states.”
There may be no greater risk to foundations, charitable giving groups or for-profit enterprise than cyber insecurity.

The question is, what should those organizations - and those that lead and manage them - be doing right now to prepare?
Agenda

- Landscape
- Threats
- Defenses
- Tips & Takeaways
Landscape
Landscape

Over 2,300 Data Breaches Disclosed So Far In 2018, Exposing Over 2.6 Billion Records

AUGUST 15, 2018 BY RBS

Risk Based Security today announced the release of its Mid-Year 2018 Data Breach QuickView report, showing there have been 2,308 publicly disclosed data compromise events through June 30th. After a surprising drop in the number of reported data breaches in first quarter, breach activity appears to be returning to a more “normal” pace. At the mid-year point, 2018 closely mirrors 2016’s breach experience but still trails the high water mark set in 2017.

~13 per day

“After a surprising drop in the number of reported data breaches in first quarter, breach activity appears to be returning to a more “normal” pace.”

Key Findings for Mid Year 2018

- 2,308 breaches have been reported through June 30, exposing approximately 2.6 billion records.
- Compared to the midway point in 2017, the number of reported breaches is down from 2,439 breaches and the number of exposed records is down from 6 billion.
- The number of disclosed instances targeting employee W-2 forms remained low, with 42 such breaches reported through Q2 2018 compared to 239 for the same time period 2017.
- The Business sector accounted for 40% of reported breaches, followed by Medical (8.3%), Government (8.2%) and Education (4.5%). Nearly 40% of breached organizations could not be definitively classified.
RISING CYBERATTACKS
The percentage of respondents affected by successful attacks has risen the last three years with no end in sight.

Source: CyberEdge Group 2017
Annual number of data breaches and records exposed (in millions) in the United States 2005 - 2016

Image via Statista.com.
Data Breach Incidents - By Type

- Insider Theft
- Hacking / Skimming / Phishing
- Data on the Move
- Accidental Email / Internet Exposure
- Subcontractor / 3rd Party / Business Associate
- Employee Error / Negligence / Improper Disposal / Lost
- Physical Theft

Source: Identity Theft Resource Center
Selected losses greater than 30,000 records (updated Sept 25, 2018)

- Equifax: 143 mil records
- Clinton Campaign: 5 mil records
- Mossack Fonseca: 11.5 mil records
- Anthem: 80 mil records
- Friend Finder: 412 mil records
- Sony Pictures: 10 mil records
- Target: 70 mil records
- Home Depot: 56 mil records
- Yahoo!: 1.5 3 bil records
What about Smaller Organizations?
“Nearly half of all cyber-attacks are committed against small businesses…

As many as 80% of small to medium sized businesses don’t have data protection of email security in place.

Small businesses – who don’t train their employees on security risks – are susceptible to the Business Email Compromise Scam (BEC), which the FBI says has led to over $3 billion in losses.”
60% of small companies go out of business within six months of a cyber attack.

58% of small businesses are concerned about cyberattacks, but more than half (51%) are not allocating any budget at all to cyber risk mitigation.

Only 38% regularly upgrade software solutions and only 22% encrypt databases.

We've collected these cyber security statistics for small businesses from various sources.

General Small Business Cyber Security Stats:
- 43 percent of cyber attacks target small business.
- Only 14 percent of small businesses rate their ability to mitigate cyber risks, vulnerabilities and attacks as highly effective.
Cybercriminals gained access to and used a valid law firm email account to email an unknown number of recipients with the subject ‘lawsuit subpoena.’

The email contained malware that attackers could use to steal banking credentials and other personal information.
<table>
<thead>
<tr>
<th>Description</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S. average cost of a data breach</td>
<td>$7.91 M ($7.3 M)</td>
</tr>
<tr>
<td>World average cost of a data breach</td>
<td>$3.86 M ($3.6 M)</td>
</tr>
<tr>
<td>World avg. per capitan (Per capita cost is the avg. cost of a lost or stolen record compromised in a data breach)</td>
<td>$148 ($141)</td>
</tr>
<tr>
<td>Per capita cost in the U.S.</td>
<td>$233 (highest; was $225)</td>
</tr>
</tbody>
</table>
FedEx has revealed the cost of falling victim to Petya to be an estimated $300 million in lost earnings.

While no data breach or data loss occurred as a result of Petya, the company previously warned that it may not be able to recover all of the systems affected by the cyber attack.
WannaCry [caused] estimated global financial and economic losses of up to $4 billion and infecting 300,000 machines around the world.

2017’s WannaCry and Petya attacks show that cybercriminals are upping their game and diversifying methods to exploit the increasing inter-connectivity of global businesses.

Total WannaCry losses pegged at $4 billion
25th September 2017 • Author: Marianne Lehnis

Ransomware attacks have reached a new peak this year, with WannaCry causing estimated financial and economic losses of up to $4 billion and infecting 300,000 machines around the world, according to Trend Micro's security and threats report.

2017s WannaCry and Petya attacks show that cybercriminals are upping their game and diversifying methods to exploit the increasing inter-connectivity of global businesses.

Trend Micro estimates that by 2018, over a million industrial robots will be employed in factories around the world; tests have shown how industrial robots can be compromised through exposed industrial networks and vulnerabilities.

This year’s systemic ransomware attacks have demonstrated that cyber crime has almost the same levels of catastrophic loss associated with natural catastrophes or some of the more traditional re/insurers cover.

The capabilities of cybercrime to disrupt the value chain on all levels will continue to drive an increase in the near-term future.

The Trend Micro report said; “Businesses still fall for email scams. According to the FBI’s Internet Crime Complaint Center (IC3) Investigation, global losses due to business email compromise (BEC) have reached $5.3 billion.
The True Cost Of Cybercrime For Businesses

© 2017 Stroz Friedberg. All rights reserved.

"...cybercrime will cost approximately $6 trillion per year on average through 2021...

...but the dollars lost only account for the direct cost of a breach... When investigating the collateral effects of a cyberattack, the outlook for businesses in the aftermath becomes bleak. Dollars and cents aside, some businesses never fully recover from a data breach...

Once a customer feels a company is unable to keep them and their personal and financial information safe, it’s game over. Security questions are [ ] a nonstarter for prospective customers.

Businesses and brands can have their reputations destroyed and their long-term viability called into question...
Cybercrime damages expected to cost the world $6 trillion by 2021

Massive expansion of the global cyber attack surface will fuel the cybercrime cost prediction for the next five years.

The cybercrime cost prediction includes damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

Cybercrime will continue its stratospheric growth over the next five years, according to a recent report published by Cybersecurity Ventures. Steve Morgan, the founder and CEO of Cybersecurity Ventures, notes that the number of attacks continues to increase at a rate of 400% per year.

While there are numerous contributors to the rise in cybercrime -- which is expected to cost the world more than $6 trillion by 2021, up from $3 trillion in 2015 -- the most obvious predictor is a massive expansion of the global attack surface which hackers target.
Landscape

- More attacks
- Against more organizations of differing size
- With increasing sophistication
- Resulting in higher costs and more serious damage to people, institutions & their causes

There is more risk today for organizations than ever before
Threats
Phishing and Spearphishing
Phishing scam

Generic email sent to a high number of recipients

Not tailored, but are engineered to appear valid

Likely uses actual company logos

Use a sense of urgency to motivate the intended action

---

Phishing scam

Generic email sent to a high number of recipients

Not tailored, but are engineered to appear valid

Likely uses actual company logos

Use a sense of urgency to motivate the intended action
Fraudsters duped this company into handing over $40 million

by Robert Hackett August 10, 2015, 4:25 PM EDT

The Ubiquiti Networks networking equipment company disclosed it lost $46.7 million through [a BEC] scam in its fourth quarter financial filing…

The company only learned about the transfers of vast sums of money (14 over a 17 day period) after being notified by the FBI…
“…authorities said the CFO of a Leoni factory [] sent the funds after receiving emails cloned to look like they came from German executives...

Investigators say the email was crafted in such a way to take into account Leoni’s internal procedures for approving and transferring funds. This detail shows that attackers *scouted the firm* in advance...

The Bistrita factory was not chosen at random either. Leoni has four factories in Romania, and the Bistrita branch is the only one authorized to make money transfers.”

Earlier this month, Leoni AG, one of the world’s largest manufacturers of wires and electrical cables, informed investors that the German company *lost almost 40 million euros* (or about $44.6 million) to online scammers. Today, we finally know how: According to investigators, the thieves simply...
Welcome back. I hope you enjoyed your holiday?

I need you to complete an outgoing wire transfer today. Will forward you the wiring instructions as soon as I have it. I'm going into a meeting soon, but I have my iPad close to frequently check my email for your response.

Regards,

Sent from my iPad.
Example Case – O365 BEC

Appears to come from Microsoft Support Team

“(7) incoming messages failed to deliver”

Inbox at 95%

“ACTION REQUIRED”

High importance

“To free up some space right now, we’ve simplified the process for you. Click below.”

Best Regards
Microsoft Support Team
Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press ‘View’ to view the list of files that have been encrypted.

Press ‘Next’ for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.
Hackers held patient data ransom, so Indiana hospital system paid $50,000

INDIANAPOLIS — An Indiana hospital system said it paid a $50,000 ransom to hackers who hijacked patient data.

The ransomware attack accessed the computers of Hancock Health in Greenfield through an outside vendor's account Thursday. It quickly infected the system by locking out data and changing the names of more than 1,400 files to "I'm sorry."
A new report from Malwarebytes released today shows a dramatic increase in the number of malware attacks U.S. small businesses face. In fact, 90 percent of small to medium sized businesses reported increased malware detection in Q1 2017 over Q1 2016. A 500 percent increase in ransomware alone was detected in March of this year in ten states.
Ransomware demands now average about $1,000 because so many victims decide to pay up.

The average ransomware attack yielded $1,077 last year, new research shows, representing a 266 percent spike from a year earlier.

The twist of the knife comes when only 47 percent of victims who pay the ransom actually recover any files.
"0000-SORRY-FOR-FILES.html’ is the ransom note which is left on the victims’ computers, after they have been infected by the latest version of SamSam ransomware. The .weapologize variant of SamSam ransomware
Insiders
In the 2016 Cyber Security Intelligence Index, IBM found that 60% of all attacks were carried out by insiders. Of these attacks, three-quarters involved malicious intent, and one-quarter involved inadvertent actors.
Defenses
Defenses

+ Plans, Policies & Programs
+ Relationships
+ Test, Assess & Drill
+ Culture
+ Risk Transfer
Plans, Policies & Programs

• Develop an actionable, up-to-date incident response (IR) plan before an intrusion occurs

• Develop and adopt a formal information security (infosec) program and policy document

• Working with IT, develop detailed data loss prevention (DLP), disaster recovery (DR) and business continuity plans (BCP)
Relationships

• Identify, select and negotiate an **IR retainer agreement** with a technical provider

• Select a law firm partner

• Establish a relationship with a PR firm

• Get to know law enforcement
Test, Assess & Drill

• Test your IR plan with **tabletop exercises**
• Penetration testing
• Red team testing
• Vulnerability, maturity assessments
• **IR readiness assessments**
• Phishing, USB key drops
It’s good to focus on firewalls, malware defenses and data protection, but too often employees are an afterthought.

- Mandatory training
- Awareness campaigns
- Monthly e-mails to the team about the latest threats, best practice reminders
- Leadership engagement...
More upper level participation needed as data breaches increase, study

As the number of data breaches increases, a recent study found 52 percent of the companies surveyed had experienced a breach, an increase from 49 percent, and despite the increase, it appears that execs are not as involved as they should be in data breach planning.

The study queried 619 executives and staff employees who work primarily in privacy, compliance and IT security in the United States and found that despite the likelihood of a breach occurring, many company leaders aren’t actively engaged and avoid responsibility for the effectiveness of their data breach preparedness plan, according to the Ponemon Institute’s Fourth
Risk Transfer (Cyber insurance)

What is cyber insurance and why you need it

Cyber insurance can't protect your organization from cybercrime, but it can provide financial footing should a significant security event occur.

A cyber insurance policy [a/k/a cyber risk insurance or cyber liability insurance coverage (CLIC)], is designed to help an organization mitigate risk exposure (through risk transfer) by offsetting costs involved with recovery after a cyber-related security breach or similar event.
Tips & Takeaways
Cybersecurity Tips & Takeaways
(General)

1. Change default settings, including admin account/password, as soon as you put new equipment / gadgets into service.

2. Don’t use a thumb drive from an unknown source; it may contain malware!

3. Close browsers immediately after use, frequently delete website search history.

4. Think before you click / don’t click a web link that is embedded in an email.

5. Confirm the email address by hovering over the sender’s name, even if it is from a trusted person.
6. Never assume an email is legit if the email asks you to download a file that does not make sense, asks you to send money, or send info.

7. Use phrases as passwords rather than 4-8 numbers, symbols and/or letters & change passwords frequently.

8. Use security questions where the answers cannot be discovered by public records, or by looking at your LinkedIn/FB page.

9. Don’t give out your SSN and date of birth at the same time.

10. Use IPS/IDS prevention software.
Cybersecurity Tips & Takeaways (for the workplace)

1. Have an incident response plan

2. Train employees

3. Back up your files – if you suffer a ransomware attack, you can refuse to pay and restore your files/system to your latest backup.

4. When you walk away from your computer at work, log out!

5. Always be wary of / double check emails from a “CEO” or “President” (roughly 1/2 of all BEC scams come from a “CEO” or “President”).
6. Train your people to be wary of phone calls seeking info – these “low tech” attacks often are advance scouting work of an impending cyberattack or spear phish.

7. Don't assume you can visit a website, not click on anything, and be “safe.” “Drive by” attacks can still install malware on your PC!

8. Use multi-factor authentication tools.

9. Ask about encryption tools that might work for you & your organization.

10. Always report suspicious emails, websites, to IT/HR folks.
Cyber Insecurity
What you Can do Now to Help Keep Your Organization Safe

John Ansbach, JD, CIPP-US
@johnansbach
jansbach@strozfriedberg.com

STROZ FRIEDBERG