

# Cyber Security 101

Community Action Partnership of Utah

Thursday, June 25, 2020

Melanie Lockwood Herman, Executive Director  
Nonprofit Risk Management Center  
**Melanie@nonprofitrisk.org**  
703.777.3504

1

## Agenda

1. What is Cyber Security?
2. Creating a data security culture
3. Train the team!
4. Data Breach Basics

2

## What is Cyber Security?

- “Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security.”

SOURCE: <https://usa.kaspersky.com/resource-center/definitions/what-is-cyber-security>

3

## What's a Data Breach?

- “an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so.”
  - Data breaches may involve payment card information (PCI), personal health information (PHI), personally identifiable information (PII), trade secrets, or intellectual property.

SOURCE: TechTarget

4

## What is PII?

(personally identifiable information)

- Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

5

## What Laws?

- In the U.S., no single federal law regulates the protection of PII; there is a complex patchwork system of federal and state laws, sector-specific regulations, common law principles, and self-regulatory programs developed by industry groups.
  - HIPPA – health care and health plan info
  - CAN SPAM Act – commercial emails
  - COPPA – online collection of info from children under 13

6

## Security Breach Notification Laws

- All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information.
- Security breach laws typically have provisions regarding:
  - who must comply with the law (e.g., businesses, data/ information brokers, government entities, etc);
  - definitions of “personal information” (e.g., name combined with SSN, drivers license or state ID, account numbers, etc.);
  - what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and
  - exemptions (e.g., for encrypted information).

SOURCE: NCSL

7

## Read up on your state’s law!

- <https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>

**Effective 5/14/2019**

**13-44-102. Definitions.**

As used in this chapter:

- (1) (a) "Breach of system security" means an unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information.
  - (b) "Breach of system security" does not include the acquisition of personal information by an employee or agent of the person possessing unencrypted computerized data unless the personal information is used for an unlawful purpose or disclosed in an unauthorized manner.
- (2) "Consumer" means a natural person.
- (3) "Financial institution" means the same as that term is defined in 15 U.S.C. Sec. 6809.
- (4) (a) "Personal information" means a person's first name or first initial and last name, combined with any one or more of the following data elements relating to that person when either the name or date element is unencrypted or not protected by another method that renders the data unreadable or unusable:
  - (i) Social Security number;
  - (ii) (A) financial account number, or credit or debit card number; and  
(B) any required security code, access code, or password that would permit access to the person's account; or
  - (iii) driver license number or state identification card number.
  - (b) "Personal information" does not include information regardless of its source, contained in federal, state, or local government records or in widely distributed media that are lawfully made available to the general public.
- (5) "Record" includes materials maintained in any form, including paper and electronic.

8

## Cyber Security Categories

- *Network security*: securing a network from intruders
- *Application security*: protecting software and devices from threats
- *Information security*: protecting the integrity and privacy of data
- *Operational security*: processes and decisions for handling and protecting data
- *Disaster recovery*: how an organization responds to a cyber security incident

9

## What's the Risk?

- 62% of businesses experienced phishing and social engineering attacks in 2018. ([Cybint Solutions](#))
- 68% of business leaders feel their cybersecurity risks are increasing. ([Accenture](#))
- Data breaches exposed 4.1 billion records in the first half of 2019. ([RiskBased](#))

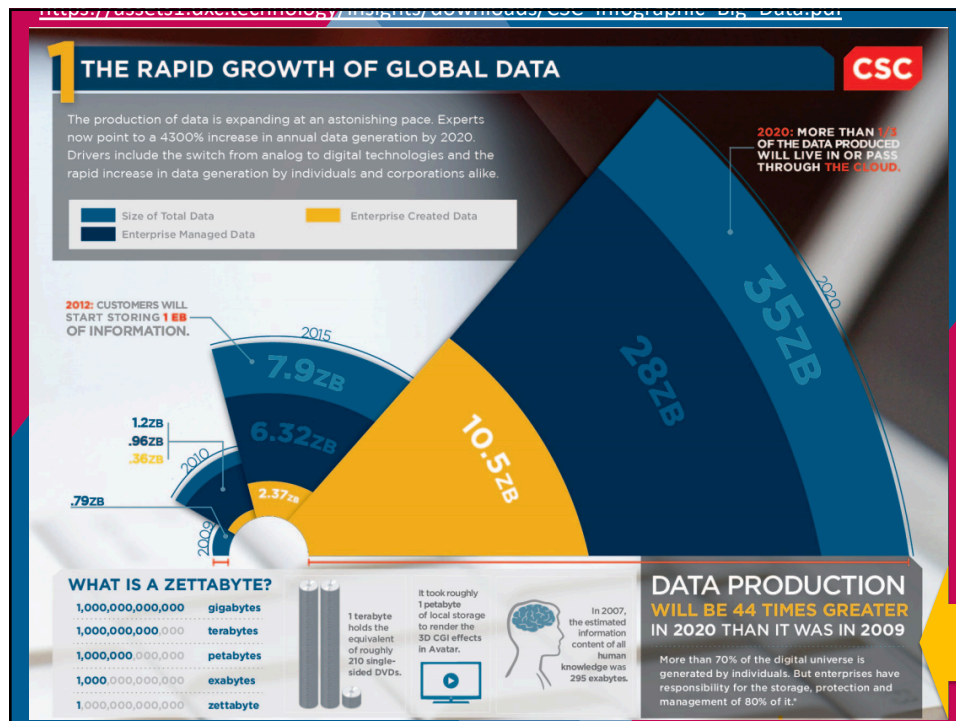
10

## More Digital Data, Less Paper

- By December 31, **2022**, all permanent records in **Federal** agencies will be managed electronically to the fullest extent possible. More electronic data, more possible breaches...
- But **Some Good News** – less paper, less paper problems...less chance of paper Personally Identifiable Information and Personal Health Information breaches.

SOURCE: Greg Walters, Peace Corps

11



12

## Whose conduct are you MOST worried about?

- Hackers/scammers
- Employees
- Other?

13

## Threat/Attack Types

- **Phishing:** 78% of all cyber espionage incidents in 2019 were related to phishing
- **Remote Worker Endpoint Security:** in 2020, 25% of all data breaches will involve off-premises assets, mobile devices and telecommuters
- **Cloud Jacking:** attacks to eavesdrop, take control of or modify sensitive files and data stored in the cloud
- **Ransomware:** experts predict an increase in sophisticated ransomware attacks
- **Deepfakes:** use of AI to manipulate an image or video to portray an activity that didn't actually happen
- **Mobile Malware:** malicious software that targets mobile phones
- **Insider Threats:** 34% of breaches involve internal actors; malicious attacks, negligent use of systems and data by employees

14

# Ransomware



Image via ZDNet.

15

# Malware

## Warning!

Your computer might be infected with spyware or adware !!!

Strange homepage, popups, **loss of important data** and unstable functioning are the sure signs that you are infected.

**Click here** to get the latest spyware removal software.

Your computer is still vulnerable to new attacks !!!

Image via OnlineCMag.

16



# Phishing

**PayPal**

## We need your help

Your account has been suspended, as an error was detected in your informations. The reason for the error is not certain, but for security reasons, we have suspended your account temporarily

We need you to update your informations for further use of your PayPal account.

[Update your information](#)

You are currently made disabled of :

- Adding a payment method
- Adding a billing address
- Sending payment
- Accepting payment

17

# Denial of Service

## Service Unavailable

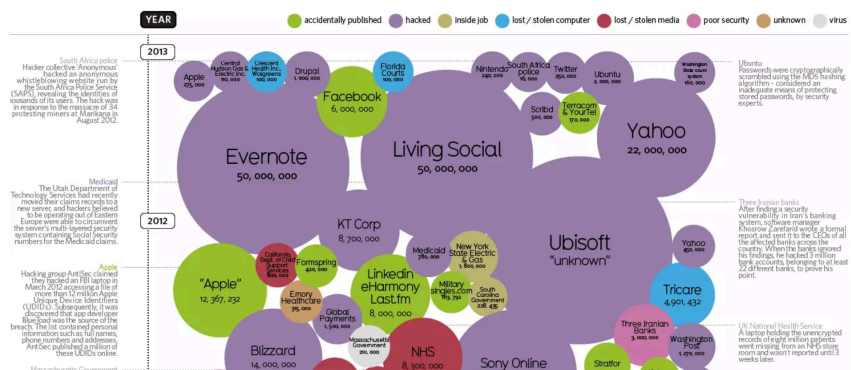
HTTP Error 503. The service is unavailable.

18

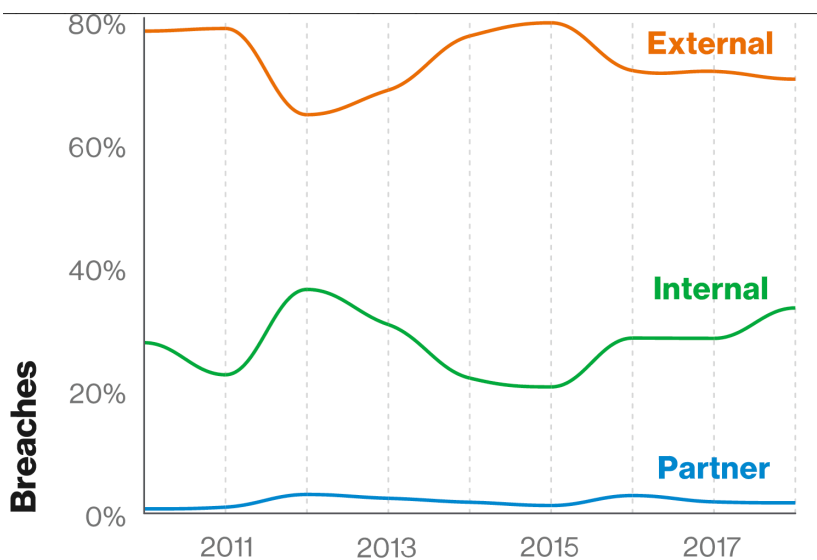
<https://digitalguardian.com/blog/history-data-breaches>

### World's Biggest Data Breaches

Selected losses greater than 30,000 records



19



**Figure 6.** Threat actors in breaches over time

20

## CYBERSECURITY STATISTICS TO DRIVE SECURITY ENHANCEMENTS NOW

A cyberattack is a scary event. It can shut down your business, cripple government agencies and incapacitate hospitals and other healthcare providers.

Here are seven cybersecurity statistics and recommendations that will get you thinking about new ways to enhance your IT security posture.



### 7 Scary Cybersecurity Statistics and Recommendations to Improve Security

1

**43% OF SECURITY BREACHES AFFECT SMBs**

In 2020, small and medium-sized businesses will continue to be primary targets of cyberattacks. Many businesses struggle with IT budget constraints and lack proper cybersecurity resources, which hackers routinely take advantage of.

Source: 2019 Data Breach Investigation Report, Verizon

**Recommendation:** Automate patch management to stay up to date with security patches. In the Kaseva 2019 State of IT Operations survey, only 42% of organizations had, or planned to have, automated patching.

SOURCE:

21

**29% OF BREACHES IN 2018 INVOLVED THE USE OF STOLEN CREDENTIALS**

Compromised passwords are a major threat to businesses. Passwords can be hacked with brute force attacks, stolen through email phishing scams and purchased on the dark web.

Source: 2019 Data Breach Investigation Report, Verizon

**Recommendation:** Tighten your password security protocols and implement authentication methods like two-factor authentication (2FA) and single sign-on (SSO) for enhanced security. Organizations also need dark web monitoring to proactively check whether their compromised credentials are being shared on the dark web. With dark web monitoring, organizations can take steps to prevent a data breach from occurring.

2

3

**3.5 MILLION UNFILLED CYBERSECURITY JOBS PREDICTED BY 2021**

The cybersecurity skill gap is a major threat to organizations. 53% of organizations report a problematic shortage of cybersecurity skills.

Source: Cybersecurity Jobs Report, Cybersecurity Ventures

**Recommendation:** Address the skill gap by implementing cybersecurity training or partner with academic institutions to nurture cybersecurity talent.

**ON AVERAGE, SMALL COMPANIES LOSE OVER \$100,000 PER RANSOMWARE INCIDENT**

Ransomware has been on the rise over the past couple of years, knocking out some city services and forcing others to revert to paper records. The effects of a ransomware attack can be very damaging to small or midsize businesses and the expensive nature of these attacks can be attributed to costs associated with downtime and recovery.

Source: Second Annual State of Ransomware Report, Osterman Research

**Recommendation:** Implement a reliable Backup and Disaster Recovery (BDR) solution that automatically tests backups to ensure recovery. Choose a BDR solution that is integrated with your endpoint management tool.

4

22

**29% OF BREACHES IN 2018 INVOLVED THE USE OF STOLEN CREDENTIALS**  
2

Compromised passwords are a major threat to businesses. Passwords can be hacked with brute force attacks, stolen through email phishing scams and purchased on the dark web.  
Source: 2019 Data Breach Investigation Report, Verizon

**Recommendation:** Tighten your password security protocols and implement authentication methods like two-factor authentication (2FA) and single sign-on (SSO) for enhanced security. Organizations also need dark web monitoring to proactively check whether their compromised credentials are being shared on the dark web. With dark web monitoring, organizations can take steps to prevent a data breach from occurring.

**3**  
**3.5 MILLION UNFILLED CYBERSECURITY JOBS PREDICTED BY 2021**

The cybersecurity skill gap is a major threat to organizations. 53% of organizations report a problematic shortage of cybersecurity skills.  
Source: Cybersecurity Jobs Report, Cybersecurity Ventures

**Recommendation:** Address the skill gap by implementing cybersecurity training or partner with academic institutions to nurture cybersecurity talent.

**ON AVERAGE, SMALL COMPANIES LOSE OVER \$100,000 PER RANSOMWARE INCIDENT**  
4

Ransomware has been on the rise over the past couple of years, knocking out some city services and forcing others to revert to paper records. The effects of a ransomware attack can be very damaging to small or midsize businesses and the expensive nature of these attacks can be attributed to costs associated with downtime and recovery.  
Source: Second Annual State of Ransomware Report, Osterman Research

**Recommendation:** Implement a reliable Backup and Disaster Recovery (BDR) solution that automatically tests backups to ensure recovery. Choose a BDR solution that is integrated with your endpoint management tool.

23

# Creating a Data Security Culture



24



## What is culture?

“what happens when people are left to their own devices.”

- Tim Ferriss, entrepreneur, author

25

## What is a data security culture?

- A *data security culture* is what happens with security when people are left to their own devices.
- For example, do they make the *right choices* when faced with whether to click on a link?
  - What are the reasons people click on suspicious links?



26

## Changing Your Data Security Culture

- The common denominator in most 3<sup>rd</sup> party attacks is **people**.
- Data security is not only about hackers: at least 25% of data security incidents have internal causes.

27

## Data Mapping

What confidential, PII + PHI does your agency collect?



28

- What kind of data do you have? Where is it located? How sensitive is the information?
- List data types by location
- Data you can't lose, data that can't be exposed, and nonessential data



29

## Technical, physical and administrative safeguards

Required by HIPAA!

- **Technical:** technology and the policy and procedures for its use that protect electronic health information and control access to it
- **Physical:** physical measures, policies, and procedures to protect systems, buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
- **Administrative:** employee training, security awareness, written policies and procedures, incident response plans, business associate agreements, and background checks.

30

## Top 10 Security Awareness Training Topics for Your Employees

1. Clean Desk Policy
2. Bring Your Own Device (BYOD) Policy
3. Data Management
4. Removable Media
5. Safe Internet Habits (phishing, pop-ups, installing software)
6. Physical Security and Environmental Controls (shoulder surfing, impersonators, leaving your computer on at night, tailgating, piggybacking)
7. Social Networking dangers
8. Email scams (phishing)
9. Malware (adware, spyware, viruses, Trojans, backdoors, rootkits...)
10. Hoaxes: "your computer will be damaged! Your data will be lost!"

<https://resources.infosecinstitute.com/top-10-security-awareness-training-topics-for-your-employees/>

31

## FUN-damentals!

- Pick a fun theme (Star Wars? Game of Thrones?) and parody it. Give gamification a try. Throw a phishing writing workshop and have your employees write a phishing email for the organization.
- Start data security briefings with a game of security trivia with a different security category each month. Hackers in the movies? Security in the news?

32



## Social Engineering

- **Hacking:** a bad actor gains access to something they shouldn't have access to
- **Phishing:** electronic communication that attempts to acquire personal or confidential information; "someone masquerades as a trustworthy source... to bait users to surrender sensitive information."
  - 30% of phishing emails are opened
  - 43% of data breaches start with phishing!

SOURCE: 2016 Verizon Data Breach Investigations Report

33

"Attackers are adept at exploiting our natural curiosity, desire to be helpful, love of a good bargain, and even our time constraints to persuade us to click."

**proofpoint.**

Security Awareness Training

# STATE OF THE PHISH

2019 REPORT



34

# Phishing: Don't Take the Bait

*Phishing* is when you get emails, texts, or calls that seem to be from companies or people you know. But they're actually from scammers. They want you to click on a link or give personal information (like a password) so that they can steal your money or identity, and maybe get access to your computer.

35

## The Bait

Scammers use familiar company names or pretend to be someone you know.

They ask you to click on a link or give passwords or bank account numbers. If you click on the link, they can install programs that lock you out of your computer and can steal your personal information.

They pressure you to act now — or something bad will happen.

36

## Avoid the Hook




**Check it out.**

- » Look up the website or phone number for the company or person who's contacting you.
- » Call that company or person directly. Use a number you know to be correct, not the number in the email or text.
- » Tell them about the message you got.

37

## Look for scam tip-offs.



- » You don't have an account with the company.
- » The message is missing your name or uses bad grammar and spelling.
- » The person asks for personal information, including passwords.
- » **But note: some phishing schemes are sophisticated and look very real, so check it out and protect yourself.**

38



### Protect yourself.

- » Keep your computer security up to date and back up your data often.
- » Consider multi-factor authentication — a second step to verify who you are, like a text with a code — for accounts that support it.
- » Change any compromised passwords right away and don't use them for any other accounts.

### Report Phishing

- » Forward phishing emails to [spam@uce.gov](mailto:spam@uce.gov) and [reportphishing@apwg.org](mailto:reportphishing@apwg.org).
- » Report it to the FTC at [ftc.gov/complaint](https://ftc.gov/complaint).



39

## Data Breach Basics



40

### 3 Tips from Jessica Ikaika

- **Put a face on your message.** Video is king as far as content goes, and crisis communication is no different. When addressing customers about a data breach or other company crisis, put your top people in the spotlight.

“Crucial Tips for Addressing and Surviving a Data Breach or Crisis,” <https://ziplineinteractive.com/blog/crucial-tips-for-addressing-and-surviving-a-data-breach-or-crisis/>

41

- **Speak, but don't forget to listen.** Making an immediate statement regarding the crisis is critical, but perhaps even more important is that you create a space to have a **conversation** with your customers.



42

- **Follow up, or you'll fall behind.** Make sure you are posting follow up statements in a timely manner. Nothing erodes trust quite like “ghosting” your customers after making your initial statement. Even if you don't have breaking news to share, simply posting a status update keeps the conversation going. For example:
  - “We are still investigating the origin of the breach. We will have another update tomorrow morning.”

43

## Data Breach Insurance

### FIRST PARTY

First-party insurance covers various expenses, including:

- Notifying all affected parties
- Costs of investigating details of the breach
- Fielding inquiries from all affected parties
- Tools to help affected parties (e.g., credit reporting)

### THIRD PARTY

- **Third-party cyber insurance** provides **liability coverage** for organizations that are responsible for a client's online security. ... If a client experiences a cybersecurity breach and sues, **third-party cyber liability insurance** can pay your legal expenses.

44

## Cyber Liability Coverage

<https://woodrufflawyer.com/cyber-liability/cyber-basics/>

- *Network security*: expenses you incur as a result of an incident
- *Privacy Liability*: liabilities arising out of a cyber incident or privacy law violations.
- *Network business interruption*: When a network of a provider that you rely on to operate, you can recover lost profits, fixed expenses and extra costs incurred during the time your business was impacted.
- *Errors and omissions*: A cyber event could keep you from fulfilling your contractual obligations; E&O covers claims arising from errors in the performance of or failure to perform your services.
- *Special endorsements*: social engineering, reputation harm, bricking

45

## Final Tips

- **Educate all staff on what data you have, where it is, how to protect it.**
- **Educate senior leadership** on changes in law and regulation and liabilities. Sell the mitigation measures: Insurance, Legal Opinions, Audits...
- **Make it quick and easy to report breaches.**
- **Focus on reporting, not punishment.**
- **Make it clear**: part of everyone's job is to report breaches.
- **Remember**: What is reported can be fixed!

46

## Resources on nonprofitrisk.org

- “Surviving and Thriving in the Wake of a Data Breach” – interview with Greg Walters from the Peace Corps - <https://nonprofitrisk.org/resources/e-news/surviving-thriving-wake-data-breach/>
- “Why People with Passwords are the Biggest Threat to Your Mission” - <https://nonprofitrisk.org/resources/e-news/social-engineering/>

47

## Additional Resources!

- RoundTable Technology – Google docs template for creating a data inventory - <https://docs.google.com/spreadsheets/d/1L1FP-ePpPLcrkYKQkuLdFHV6xj9Y-k6z4jaBQKxgKE/edit#gid=0>

Person	Information (What is this information called?)	Description	Location (Where is this information housed?)	Classification (Information)			Risks			In-place Safeguards			Recommended Mitigations
				Confidentiality	Integrity	Availability	Confidentiality	Integrity	Availability	Confidentiality	Integrity	Availability	
Jane Fundraiser	Salesforce	CRM database	Salesforce (Cloud)	medium	high	medium	password breach old user accounts MFA active	accidental deletion	Salesforce service outage internet outage	password policy MFA S&A Backup Internal Service	Sperring.com backups	Salesforce S&A Backup Internal Service	Consider two-factor authentication Regularly disable or remove old user accounts
Jane HR Rep	HR folder	Documents and spreadsheets	Internal file server	medium	medium	low	password breach network breach old user accounts MFA active	Server failure	Server failure Network outage	password policy MFA Sperring.com backups	Local backups by S&A	None	Consider migrating to cloud-based file sharing service with two-factor authentication if migrating on the server, consider adding cloud-based backup solution along with local backup solution for office
Jane Lawyer	Case Files	Random documents pertaining to confidential cases	Dropbox (Cloud)	high	high	medium	Breach of Dropbox account Breach of Dropbox (the service itself) Intended of documents in transit	Phishingware Limited retention profiles with Dropbox	Dropbox outage Internet outage	password policy MFA Sperring.com backups	Dropbox Retention	Dropbox 98.9% uptime S&A	Consider migrating to cloud-based file sharing service with two-factor authentication if migrating on the server, consider adding cloud-based backup solution along with local backup solution for office Consider adding next-gen backup tool such as Backupify to equipment Dropbox retention

48



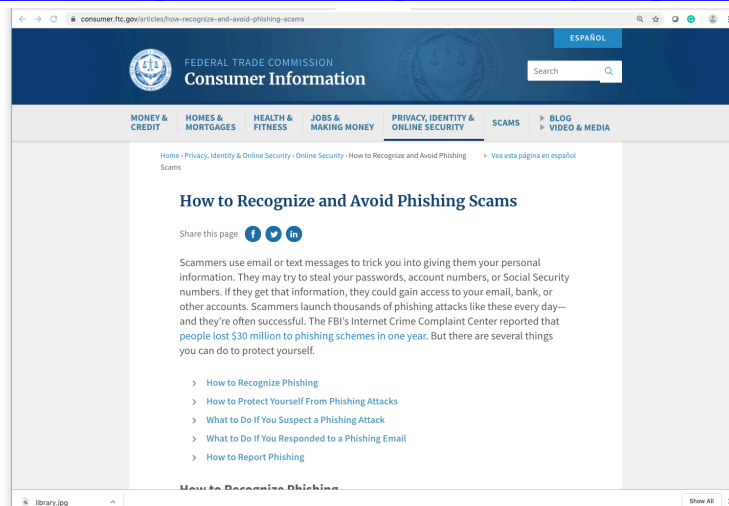
## Additional Resources

- What Nonprofits Need to Know About Security: A Practical Guide to Managing Risk – Idealware
- Email Attacks Against Nonprofits Are On the Rise. Is Your Organization Vulnerable? - Chris Bernard, April 2019 - <https://www.idealware.org/email-based-attacks-against-nonprofits-are-on-the-rise-is-your-organization-vulnerable/>
- Email Phishing Protection Guide – Enhancing Your Organization’s Security Posture - <https://blogs.technet.microsoft.com/cloudready/2018/07/31/introducti-on-email-phishing-protection-guide-enhancing-your-organizations-security-posture/>

49

## Additional Resources

[www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams](http://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams)



50

## Table of Contents

<p><b>Foreword</b>.....III</p> <p><b>Executive Summary</b>.....IV</p> <p><b>Section 1: Breaking botnets</b>.....5</p> <p style="padding-left: 20px;">Analysis and explanation.....6</p> <p style="padding-left: 20px;">Solutions and recommendations.....14</p> <p><b>Section 2: Hackers turning to easy marks</b>.....15</p> <p style="padding-left: 20px;">Social engineering.....16</p> <p style="padding-left: 40px;">Analysis and explanation.....17</p> <p style="padding-left: 40px;">Solutions and recommendations.....20</p> <p style="padding-left: 20px;">Poorly secured cloud apps.....21</p> <p style="padding-left: 40px;">Analysis and explanation.....22</p> <p style="padding-left: 40px;">Solutions and recommendations.....25</p> <p style="padding-left: 20px;">Taking advantage of legitimate platform features.....26</p> <p style="padding-left: 40px;">Analysis and explanation.....27</p> <p style="padding-left: 40px;">Solutions and recommendations.....28</p>	<p><b>Section 3: Wrestling ransomware</b>.....29</p> <p style="padding-left: 20px;">Analysis and explanation.....30</p> <p style="padding-left: 20px;">Solutions and recommendations.....34</p> <p><b>Additional noteworthy threat intelligence</b>.....36</p> <p style="padding-left: 20px;">Cloud threat intelligence.....37</p> <p style="padding-left: 20px;">Endpoint threat intelligence.....41</p> <p><b>Conclusion</b>.....52</p> <p><b>Authors and Contributors</b>.....53</p> <p><b>Data sources</b>.....54</p> <p><b>Glossary of threat definitions</b>.....57</p>
--	---

51

## Trends (Microsoft SIR Volume 23)

1. Botnets continue to impact millions of computers globally, infecting them with old and new forms of malware.
  - “A bot is a program that allows an attacker to take control of an infected computer. A botnet is a network of infected computers that communicate with command-and-control servers. Cybercriminals use botnets to conduct a variety of online attacks, such as send spam... spread malware, facilitate click fraud...”
2. Hackers went for the easy marks.
3. Ransomware is still a force to be reckoned with and doesn't look to be slowing down any time soon.

52

## Phishing Related Findings – MS SIR Vol. 23

- **More than 75% of phishing mails include malicious URLs to phishing sites.** Other variations include malicious phishing attachments and links in attachments.
- **Phishing mails impersonate popular brands**
  - Microsoft associated brands (for example, Office 365)
  - Other commonly abused brands include, but are not limited to, DocuSign, Dropbox, Apple and Amazon.
  - Recent investigations show attacks that impersonate popular courier services such as FedEx, DHL and UPS.
  - The research team also detected impersonation related to banks and government services.
- Although user impersonation and domain impersonation techniques were low in volume (number of instances in which techniques were used), they were high-severity attacks.

53

## Resources! www.nonprofitrisk.org



**Put on Your Thinking Map: Create a Contingency Map in 5 Steps**  
By Melissa Lockwood Herman

A short plane ride to Columbus on Saturday offered the ideal opportunity to catch up on overdue reading from some of my favorite weekly e-newsletters. One piece from the team at McKinsey caught my eye by combining two favorite topics in a single headline: “Risk business: 10 first-contingency planning.” The authors of the piece explain that a contingent road map helps leaders create a pathway to update strategy over time by capturing “all the changes that may occur in uncertain markets and when things go sour. Most important, they present the specific changes your company must make to its strategy under different scenarios.”

Many nonprofit leaders tell me that contingency planning is a back-burner issue in their organizations. Why? A common reason is that thoughtful contingency plans take a lot of time to draft. Add peer review and executive team approval... and a short-term project has become a behind-the-scenes. But the terrible truth about wise strategic priorities in our sector is that sometimes we choose the wrong strategy. And sometimes the world around us changes in ways that none of us



54

## Resources

- 10 Data Privacy and Encryption Laws Every Business Needs to Know - <https://securityboulevard.com/2019/06/10-data-privacy-and-encryption-laws-every-business-needs-to-know/>



[www.digitalguardian.com](http://www.digitalguardian.com)

55

<https://enterprise.verizon.com/resources/reports/dbir/>



### Understanding the threats can help you manage risk effectively.

The threats are real, the attackers motivated. But something stands between them and your organization's data: you and your security teams, with the insight, perspective, and tools to take action. You'll find that all right here.

[Download the Report](#)

[Read the Executive Summary](#)

[Contact us](#)

56



Melanie Lockwood Herman, Executive Director  
Nonprofit Risk Management Center  
**Melanie@nonprofitrisk.org**  
703.777.3504