Welcome!

Larry Deniston – CMIT Solutions of Grand Rapids and Southwest Michigan

40 years of experience designing, developing and delivering cutting-edge IT solutions using the latest technologies to Small Businesses, Non-Profits and Local Government

Scott Taber

- Cybersecurity professional passionate about raising awareness of every day cyber threats and trends.
- Prior to joining the Michigan SBDC, served as an IT Security Analyst at Ferris State University. As an IT Security Analyst, managed full disk encryption, mobile device management, Office365 security policies, and provided security awareness training through multiple platforms. Has assisted with incident response, vulnerability and risk assessments, data loss prevention, and data security access.
- Graduated from Ferris State University with a degree in Information Security and Intelligence and Criminal Justice. Also obtained a program certificate in Geographic Information Systems.

Scott Taber
tabers@gvsu.edu
Cybersecurity Awareness Specialist
MI-SBDC Lead Center

Disclaimer

Please know that if you implement the measures in this presentation, you could still be impacted.

Realities for Small Business

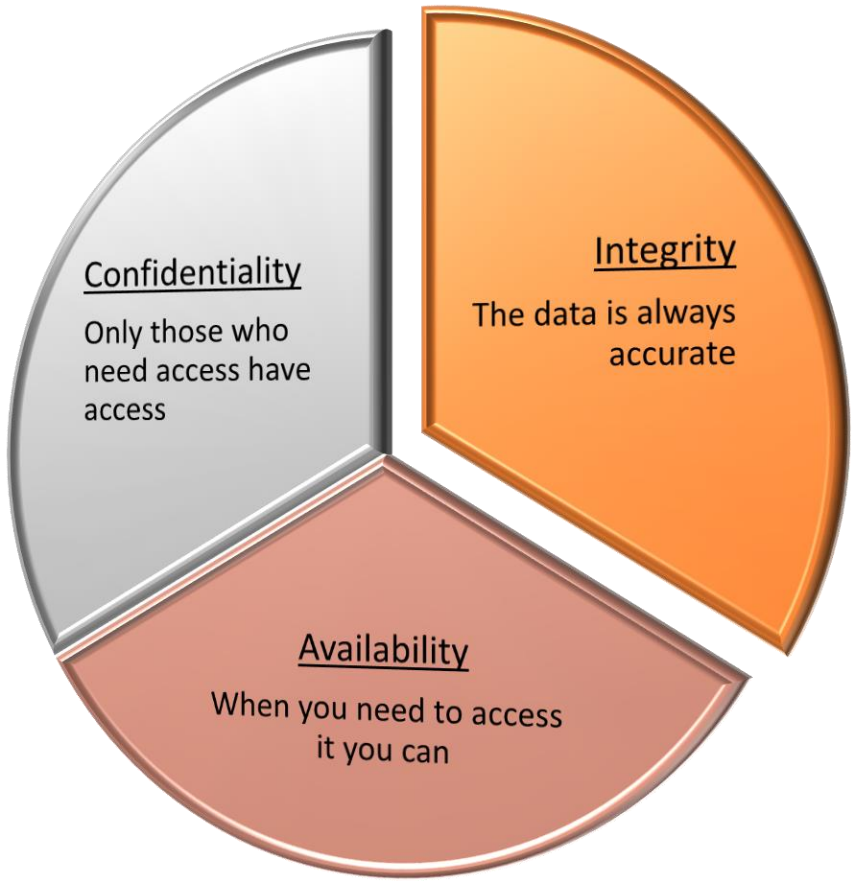
“There are only two types of companies – those that have been hacked, and those that will be.” - Robert Mueller, Former FBI Director 2012

Why this is important to you

- The level of cybersecurity directly impacts the value of the business in this always connected world

Cybersecurity is

- The practice of ensuring confidentiality, integrity, & availability (CIA Triad) of information – CSO Online 2017



Cybersecurity is

- Passwords & Multifactor Authentication
- Encryption & Virtual Private Networks
- Data Backups
- Software Updates
- Incident Response Plans
- Antivirus and Antimalware Software
- Network Security
- Mobile Device Security
- Security Policies
- Security Awareness Training

Why cybersecurity is important to small business – Access to your data

Why cybersecurity is important to small business

Source: Verizon DBIR 2019

Cyber Attacks can lead to Monetary Loss

It's not a question of *if* but *when*

39% of organizations saw a substantial loss of revenue because of a cyber- attack.

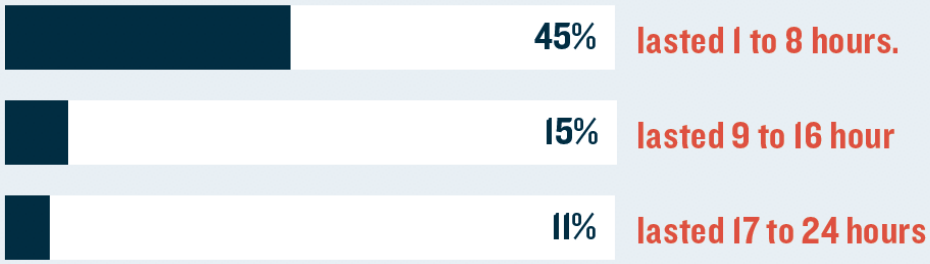
42% saw a business opportunity lost

39% saw a substantial loss of customers.

Source: Cisco 2017 Annual Cyber Security Report

An outage can shut down your business and lead to loss of productivity and income. Ensure outages are not an issue with the Cybersecurity Assessment.

Network Outages that are caused by security breaches can often have a long-lasting impact.



Source: Cisco 2017 Security Capabilities Benchmark Study

Where (locally reported complaints to BBB)?

Search for Scams

Search using any or all of the fields below.

Keyword

Scam Type

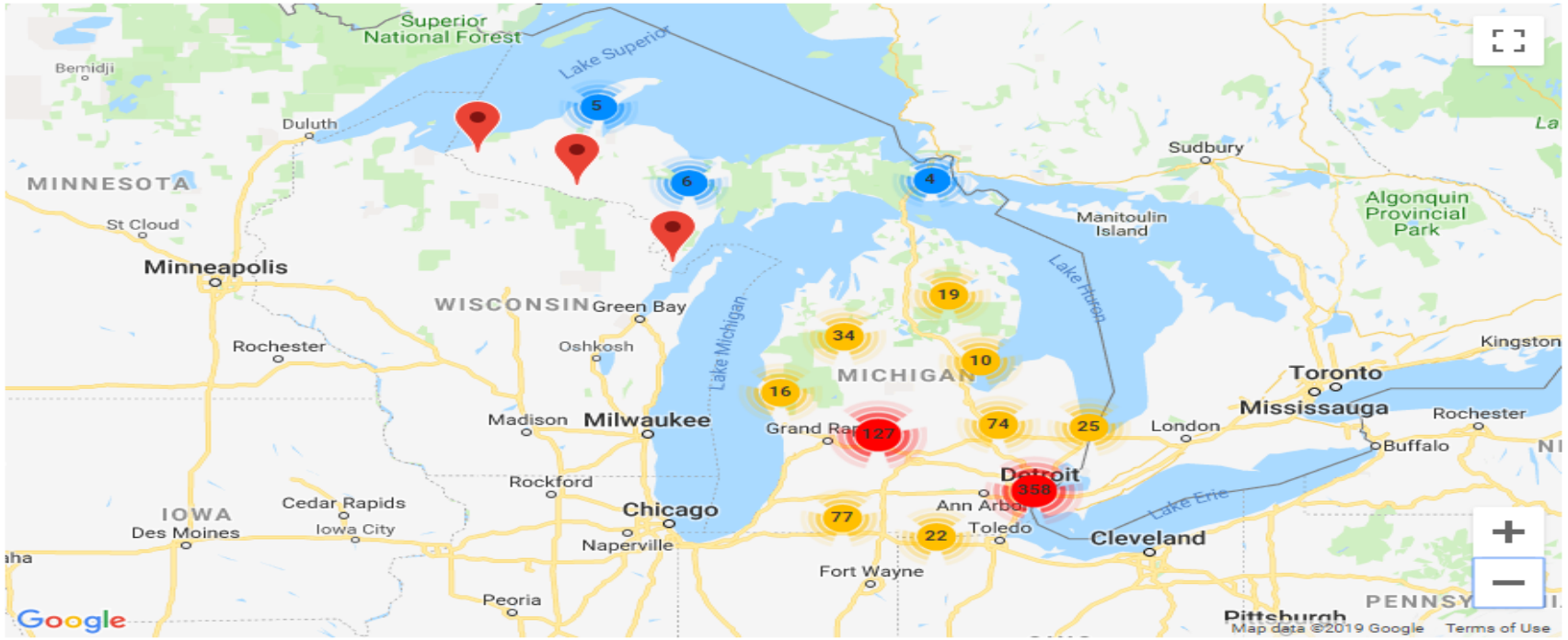
- Identity Theft
- Business Email Compromise
- Credit Cards
- Tech Support
- Phishing
- CryptoCurrency
- Online Purchase
- Nigerian/Foreign Money Exchange

Country: United States

State: Michigan

Date Reported: Jan 1, 2018 to Dec 31, 2018

780 Scams Found



Showing 500 Results Sorted by **Date**

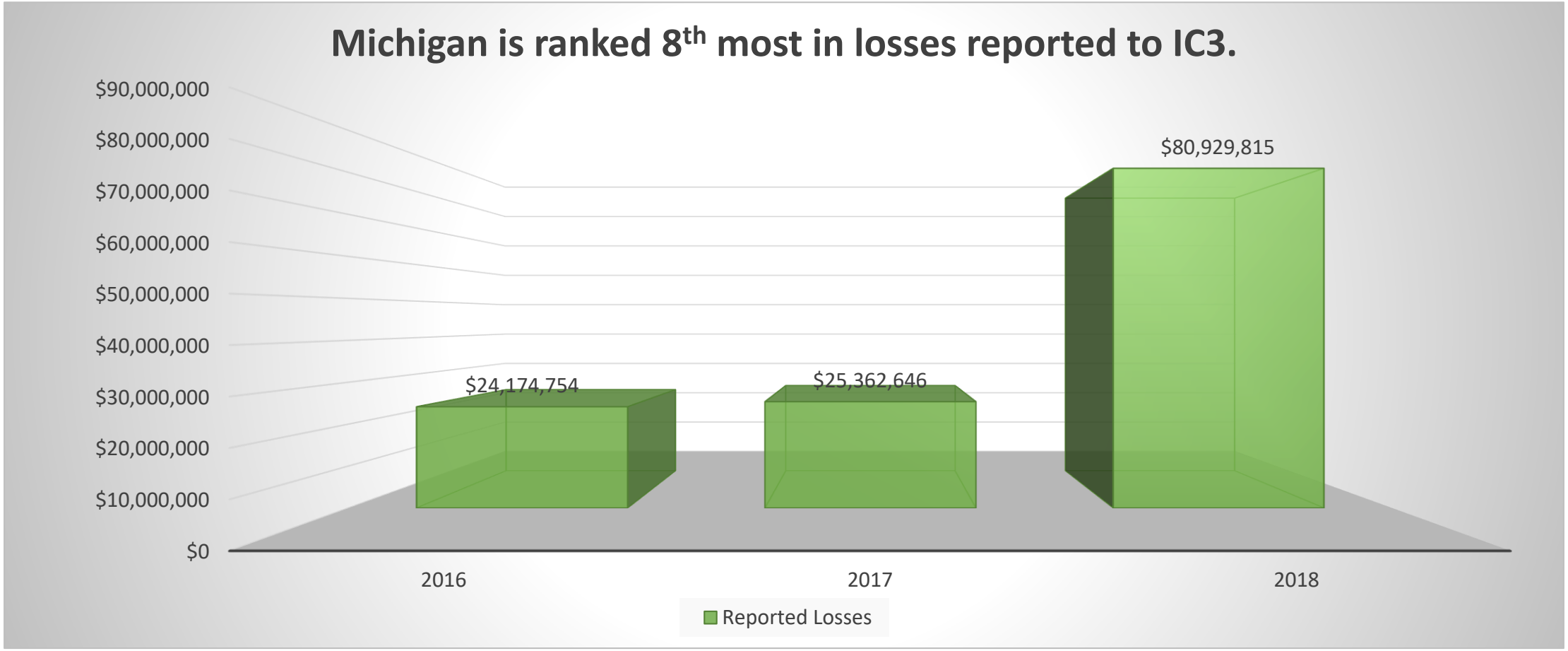
Date	Scam Type	Postal Code	Dollars Lost	Details

Source: Better Business Bureau 2019

Why cybersecurity is important to small business

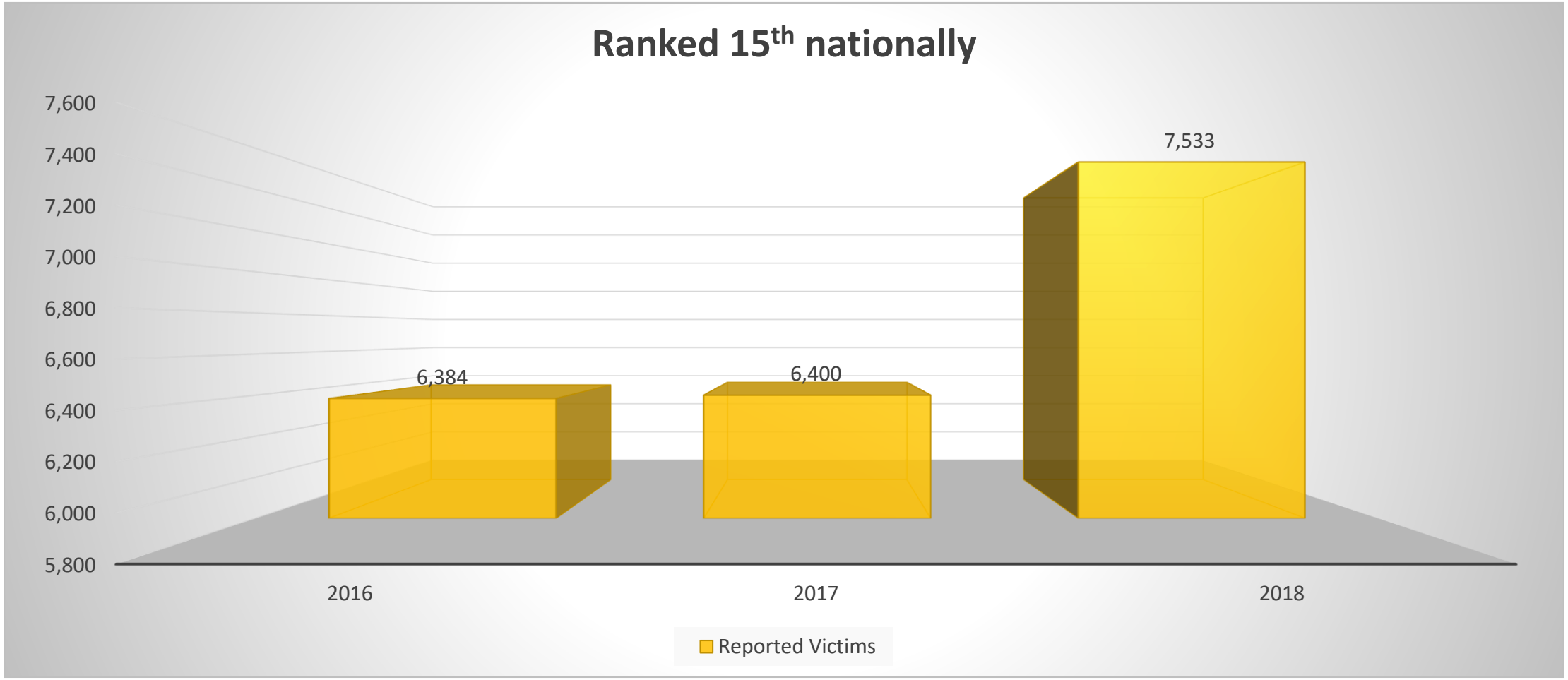
- $175B in the U.S.
  - Source: McAfee 2018
- $600B Globally
  - Source: McAfee 2018
- $6 TRILLION globally by 2021
  - Source: Cyber Security Ventures 2017
- $117,000 per breach for small businesses
  - Source: Kaspersky Lab 2017

Why cybersecurity is important to small business



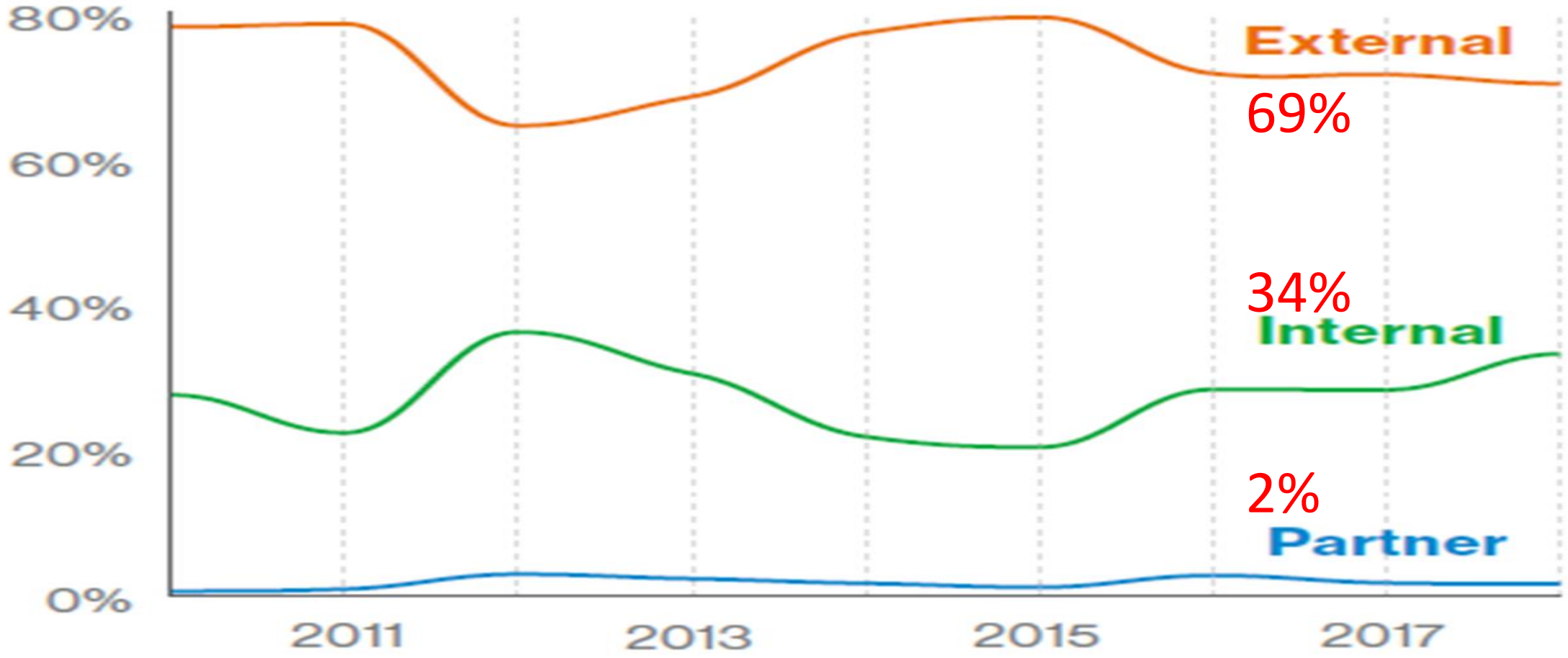
Source: Internet Crime Complaint Center 2019

Where (reported complaints to IC3 in Michigan)?



Source: Internet Crime Complaint Center 2019

Who (are the attackers)?

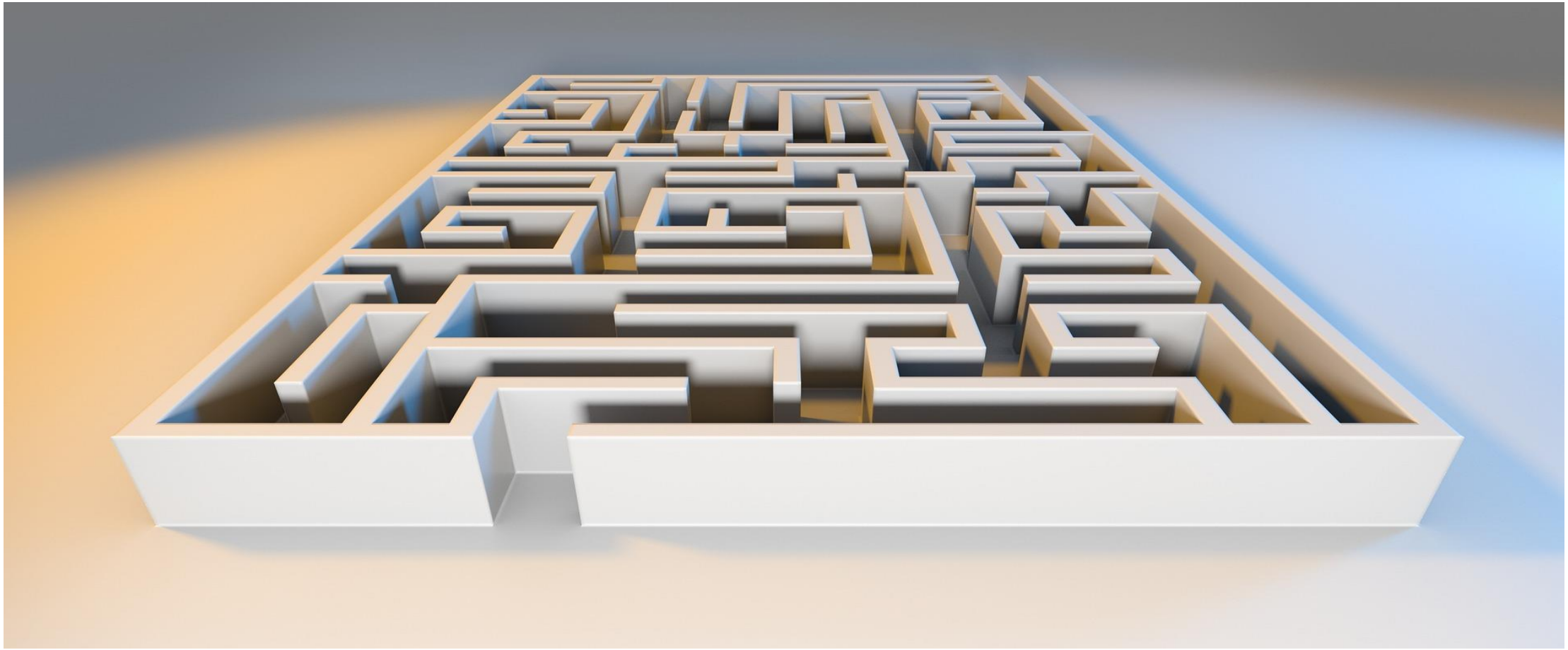


Source: Verizon DBIR 2019

Are the businesses you represent safe from Cybersecurity Threats?

1. Have they recently experienced a ransomware, malware or phishing attempt?
2. Are they unsure their company network is secure.
3. Have they recently experienced a data breach?

Not so simple



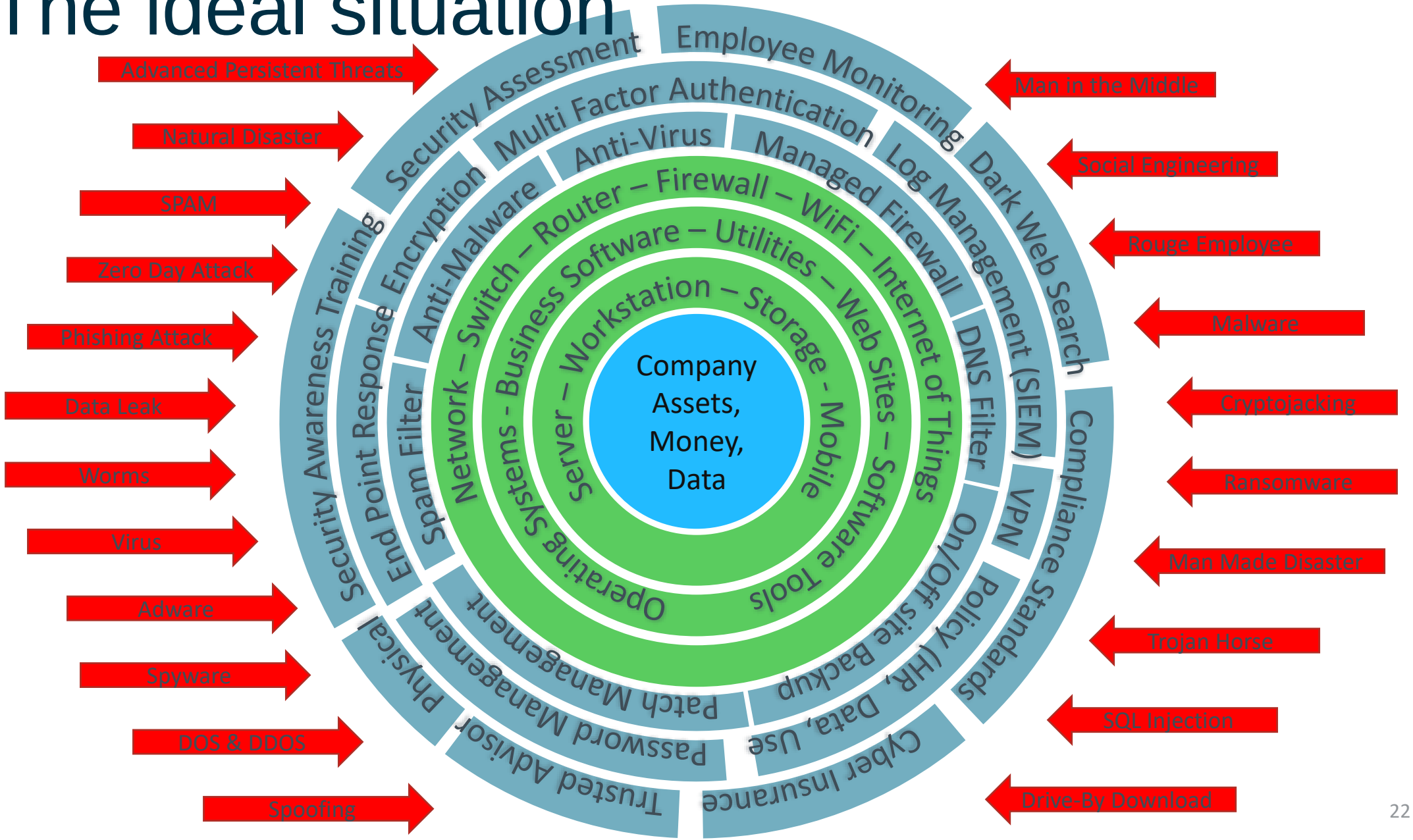
IT Security isn't as simple as you might think.

How will you…	IT services provides…	Why it matters to you
Know if your current IT provider is protecting you	"point-in-time" cybersecurity consulting engagement	Identify vulnerabilities in an organizations IT infrastructure, policies, practices, and physical environment
Know where your vulnerabilities are	Full Network scans and a control questionnaire that is validated against full inspection of your environment	Help your client understand not only their vulnerabilities, but also the whole safeguard construct regarding key areas of security
Understand where the weak points are in your infrastructure that hackers will take advantage of	Full analysis of observations and findings that our expert staff will compile and present to you	Gain a full understanding of just where potential risks exist in their IT environment
Know If you are complaint with your regulatory needs	A Cybersecurity assessment can also be tailored to address most regulatory needs – HIPAA, Sarbanes-Oxley, GDPR, DFARS, PCI DSS.	Find out where their environment is non-compliant using the National Institute of Standards and Technology, or NIST 800-53 framework
Identify what must be addressed to become compliant for your regulatory needs	A control questionnaire and scans will help us pinpoint areas where your business has fallen out of compliance	Give your client the information of what must be addressed and in what priority to become fully compliant
Start on the path to a healthy IT environment	A full Cybersecurity Assessment process will result in a number of recommendations that put you on the path to hardening your technical environment against attacks	Once the vulnerabilities in their environment have been found and analyzed, it's important that they act on the recommendations their IT services will provide. Knowing where a threat vector exists is only the first step. Once a vulnerability has been identified, get help finding solutions to implement a fully secured environment and maintain it against the ever evolving threat landscape.

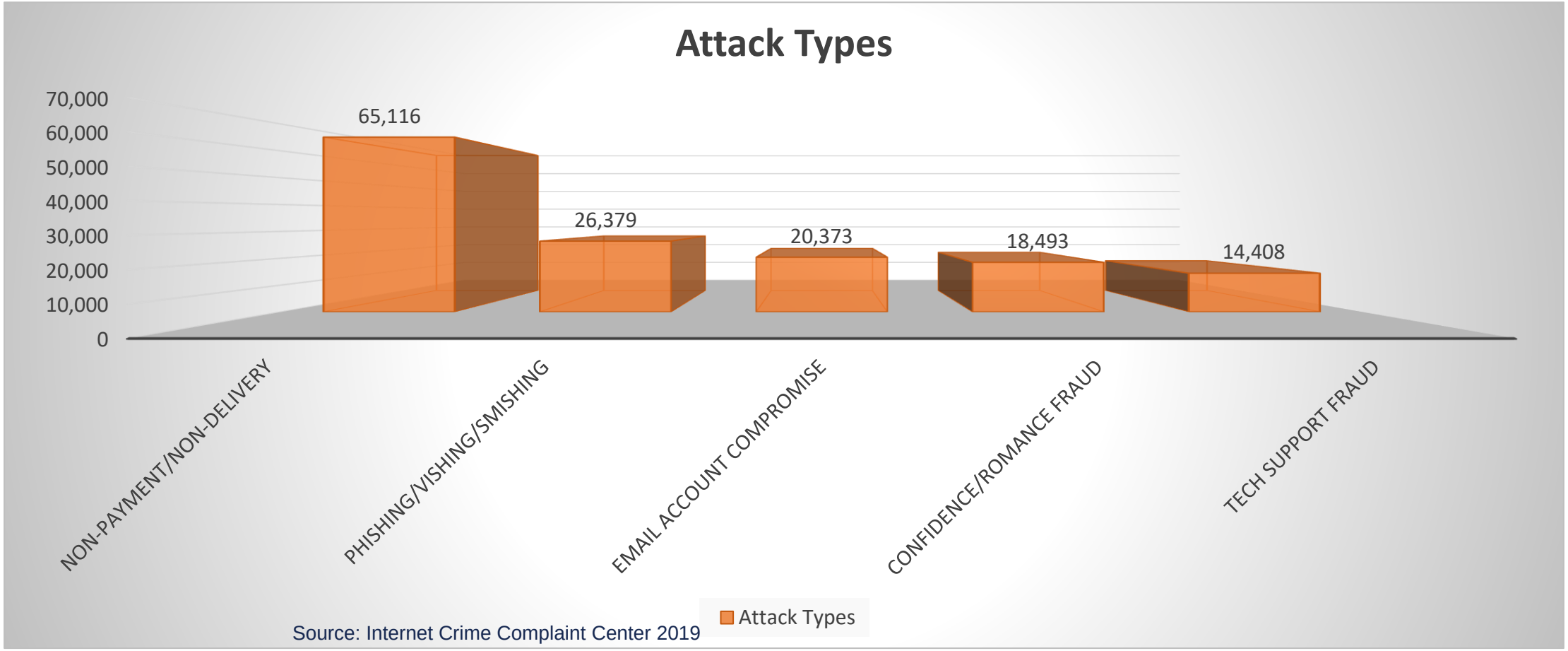
The Situation

The typical situation

The ideal situation



How (national attack types reported by IC3)?



Source: Internet Crime Complaint Center 2019

What you can do today

Basic practices (the musts)

- Backup your data daily
- Properly configure your network(s)
- Deploy anti-virus & anti-malware solutions
- Use strong user credentials
- Update software & hardware regularly
- Train yourself and employees regularly
- Business Cyber Insurance

Basic practices (the policies)

- Cybersecurity Policy
  - Formal business policy stating the process of safeguarding data & technology from corruption, loss, & compromise
- Other important cybersecurity policies
  - Acceptable Use
  - Data Classification
  - Mobile Device
  - Email
  - Clean Desk
  - Disaster Recovery
  - Data Breach
  - Data Protection

Plan and prepare

- Know your data
  - Where is your data?
    - Cloud vs Onsite
  - How does your data flow?
    - The systems and applications that use it
  - Who has access to your data?
    - Employees, vendors, managed service providers, customers
  - What kind of data do you have?
    - HR/Employee data, financial data, customer data, intellectual property

Plan and prepare

- Importance of your data
  - Know how much it costs your business to be down for
    - One hour, one day, one week
  - Understand why your data is valuable to others
    - Can it be sold on the dark web
  - Understand what can happen with your data if it is stolen
    - Loss of business, loss of reputation, cost to protect employees and customers
- Consider a Cybersecurity Assessment

Why is a Cybersecurity Assessment Important to the Sale of a Business

- Buyer
  - Know if there are issues that could be a liability
  - Know what costs would be involved in remediating issues
  - Use issues as a Price negotiating point

- Seller
  - Provide buyer with assurance there are no costly issues to be dealt with
  - Know before the buyer does so it doesn’t become a price negotiating issue
  - Find issues before they ruin your business

Your Options, a Cybersecurity Assessment

The CMIT Cybersecurity Assessment™ is offered in various regulatory and non-regulatory versions, with features as shown in the following table:

Version	Type of business
General Business [non-regulatory	Most small to medium businesses concerned about security, but have no compliance needs
HIPAA - Health Insurance Portability and Accountability Act or HIPAA	Covered Entities or Business Associates in the medical field
PCI DSS - Payment Card Industry Data Security Standard or PCI DSS	Collects and stores credit information of their clients
DFARS - Defense Federal Acquisition Regulations Supplement	Must maintain federal or governmental standards when contracted by the government
GDPR - General Data Protection Regulation	European standards for the protection of individual private data
Full NIST 800-171 Control Questionnaire	The complete standards from special publication “Protecting Unclassified Information in Nonfederal Information Systems and Organizations”

Thanks!

Larry Deniston
CMIT Solutions, your technology team
(616) 419-8838
ldeniston@cmitsolutions.com
cmitsolutions.com

Thank You!

- Scott Taber
- Cybersecurity Awareness Program Specialist
- Michigan Small Business Development Center
- tabers@gvsu.edu
- https://sbdcmichigan.org/