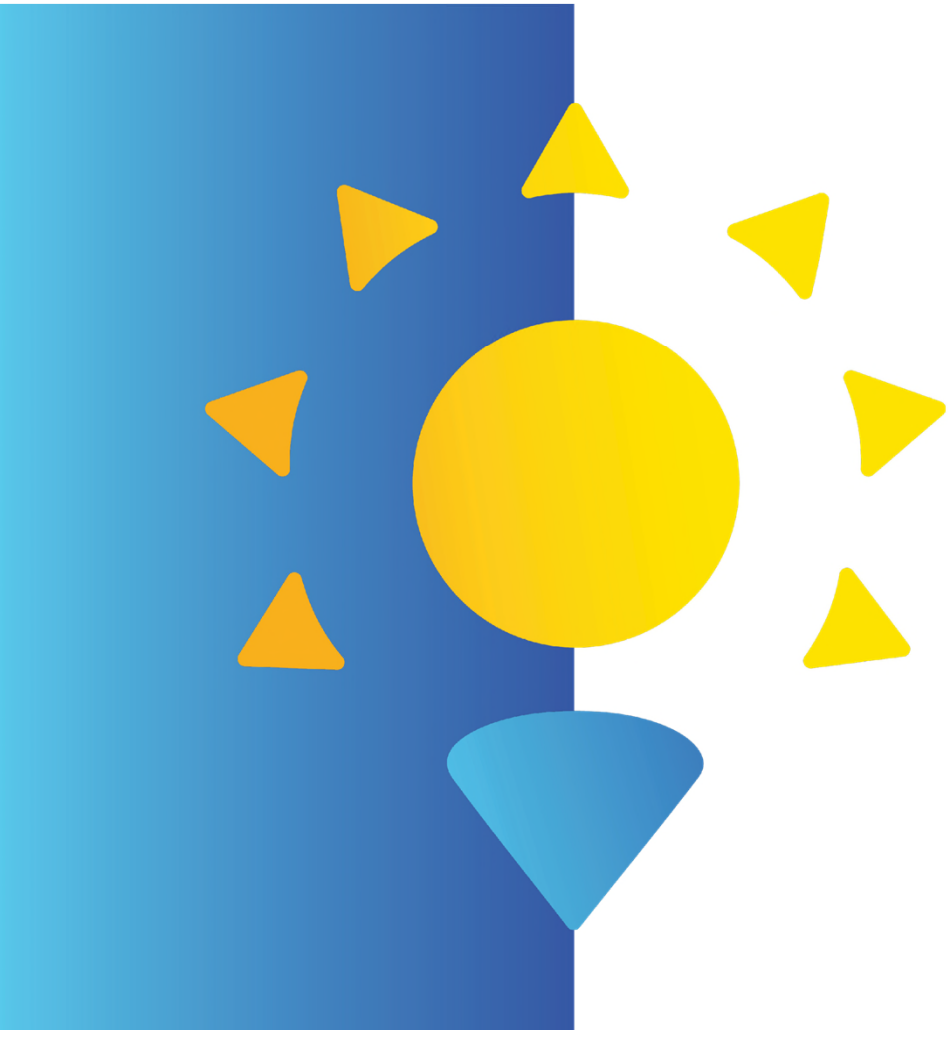


FLC FLORIDA LEAGUE OF CITIES

Cyber Attacks: Impacts & Remediation Strategies

LOCAL VOICES MAKING LOCAL CHOICES

Cyber Attacks: Impacts & Remediation Strategies

FLGISA
FLORIDA LOCAL GOVERNMENT INFORMATION SYSTEMS ASSOCIATION

Michael J. van Zwieten, CGCIO, MCSE
Director of Technology Services, Florida League of Cities
Executive Director, FLGISA

FLC
FLORIDA LEAGUE OF CITIES

FLC
FLORIDA LEAGUE OF CITIES

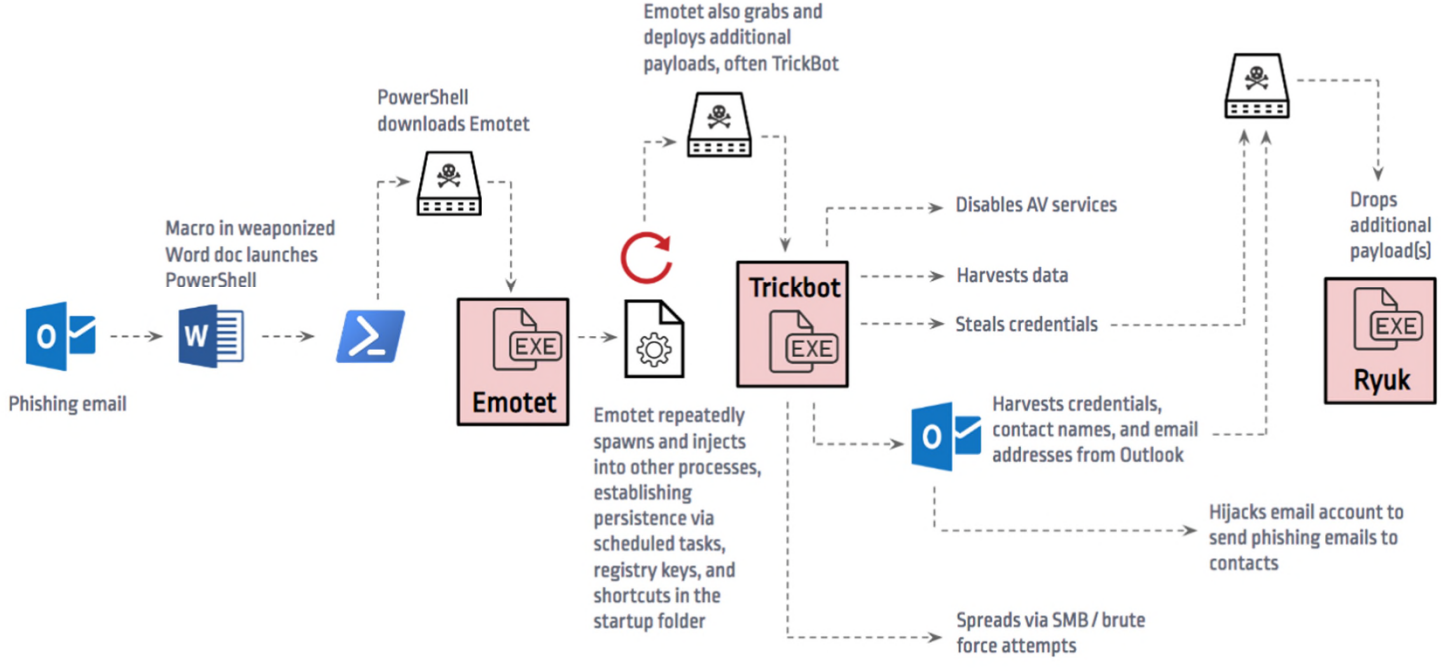
Ransomware... what is it?

- Malicious form of software that encrypts most files on a network's local computers and servers, demanding a ransom if you want the files back; most commonly paid in bitcoin.
- **NEW DEVELOPMENT**: Hackers are now also downloading your data and extorting you to pay a ransom or this information will be exposed to the public.
- 90%-95% of successful attacks come through email (FBI)
- It only takes *1* click on a malicious link by an employee to take down an entire organization.
- There are NO magic bullets that can prevent a Ransomware event … but several less-magical best practices will.

FLC
FLORIDA LEAGUE OF CITIES

Ransomware... how does it work?

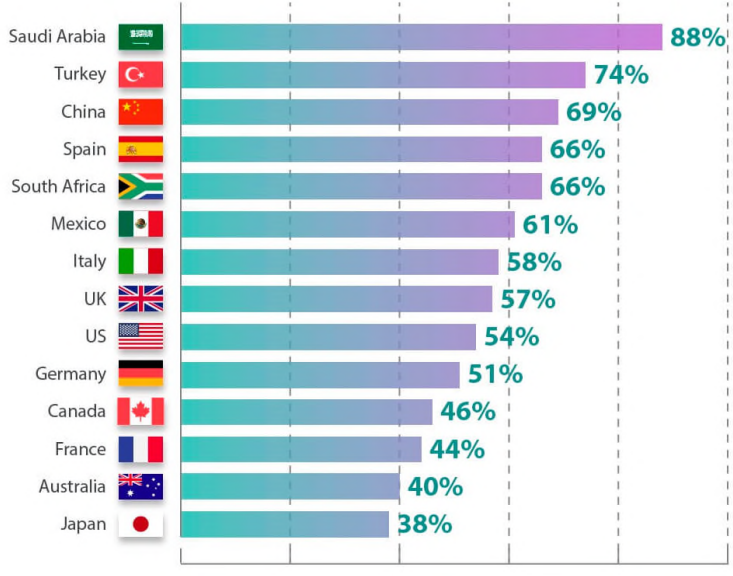
Emotet Trojan: Attack Diagram



FLC
FLORIDA LEAGUE OF CITIES

Ransomware... who is affected?

HOW MANY ORGANIZATIONS REPORTED RANSOM ATTACKS IN THE LAST YEAR?

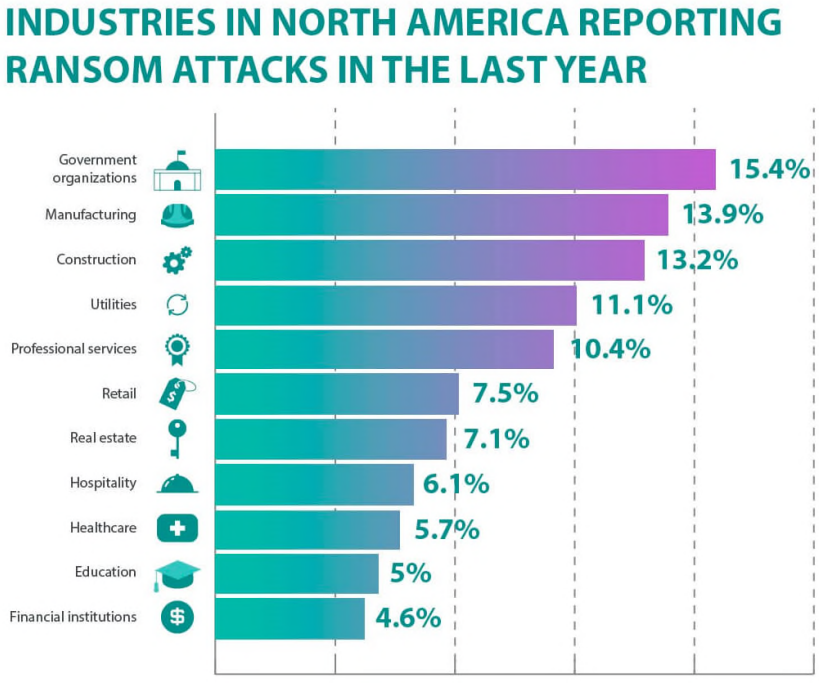


Percentage of security professionals at medium and large organizations who responded that they were affected by ransomware within a 12 month period.

SafetyDetectives Q2 2020

FLC
FLORIDA LEAGUE OF CITIES

Ransomware... who is affected?

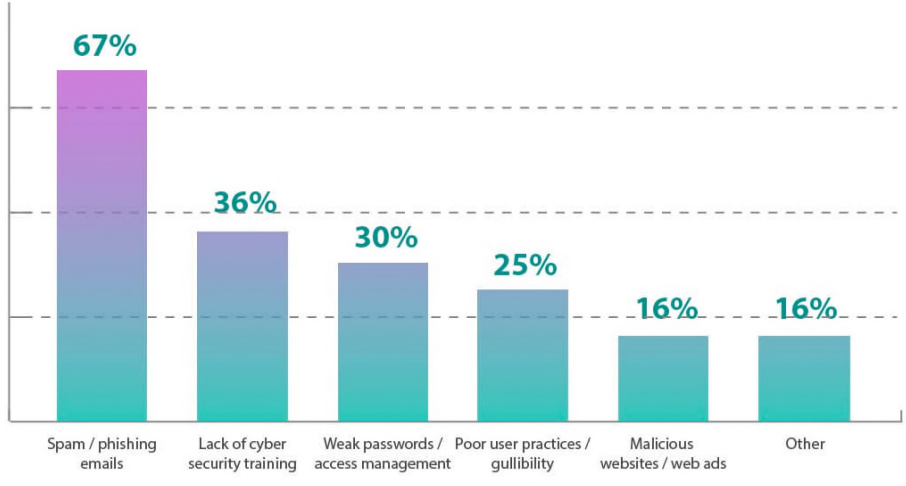


SafetyDetectives Q2 2020

Ransomware... who is affected?

MOST COMMON METHODS OF RANSOMWARE INFECTIONS IN NORTH AMERICA

Based on MSPs reporting attacks on organizations. (Some were targeted by more than one method.)

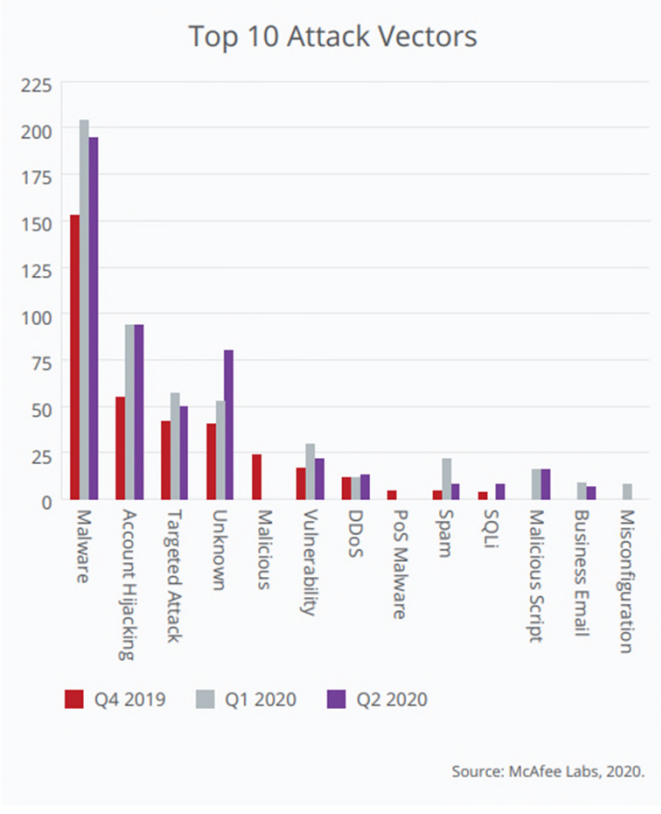


Managed Service Providers were asked which were the most common ransomware delivery methods they've seen for their clients in 2019.

SafetyDetectives Q2 2020

FLC
FLORIDA LEAGUE OF CITIES

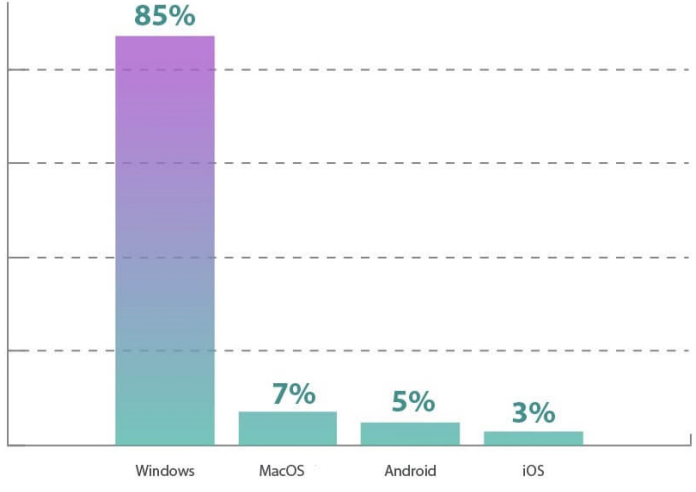
Ransomware... who is affected?



- 419 threats per minute in Q2 2020, up 12% from Q1
- PowerShell malware increased 117% over Q1 2020
- New Office malware increased 103% over Q1 due to documents spawning PowerShell
- New Linux malware increased 22% over Q1

Ransomware... who is affected?

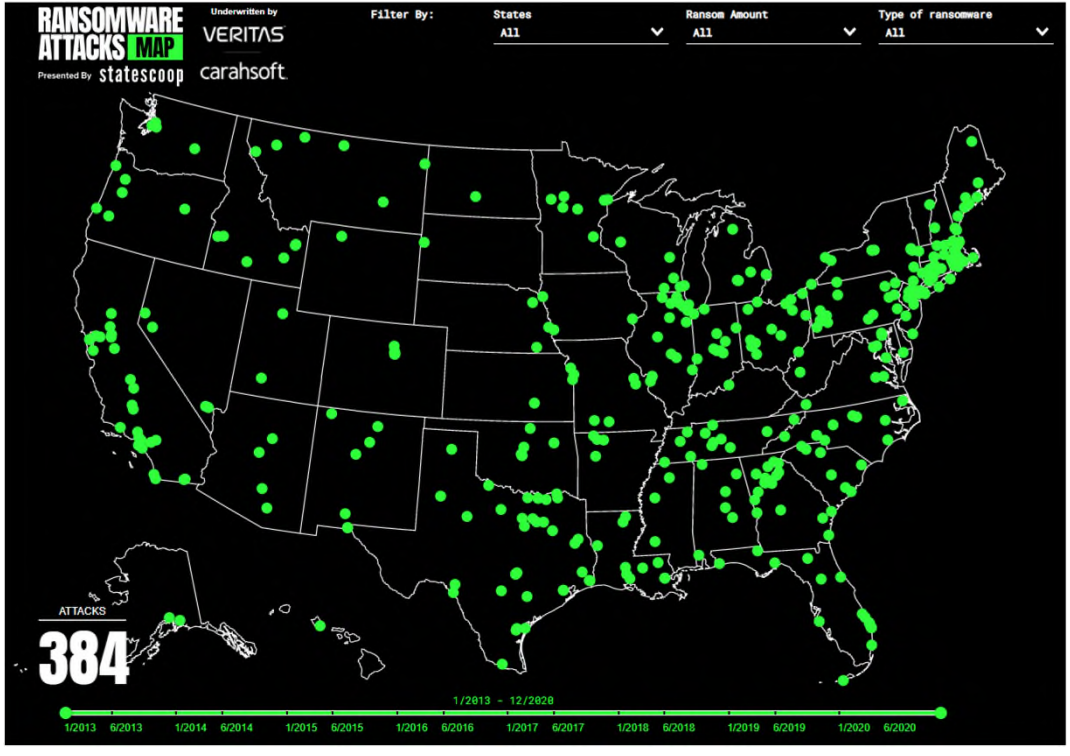
SYSTEMS TARGETED MOST BY RANSOMWARE



SafetyDetectives Q2 2020

FLC
FLORIDA LEAGUE OF CITIES

Ransomware... who is affected?



- 200+ attacks in the last 2 years alone
- Municipal Governments have become a prime target after the large payouts in FL in 2019
- Baltimore 2019 – Didn't pay $76K - Cost $18.2M
- Atlanta 2019 – Didn't pay $51K – Cost $17M
- New Orleans 2019 – Didn't pay – Cost $7M
- Texas 2019 – 22 Cities on MSP – may have paid $2.5M in ransom

Statescoop.com Q4 2020

Ransomware... who is affected?

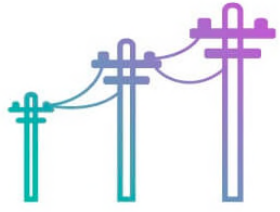
FUTURE PREDICTED TRENDS IN RANSOMWARE ATTACKS

IoT devices

IoT devices will become a more prominent attack vector

Social media

While social networks beef up internal security, tainted links targeting users will increase in numbers



Utility infrastructure

Critical infrastructure will be targeted more, in efforts to have a better chance of ransom payment.

Managed service providers (MSPs) were asked how they predict ransomware will target its victims in the future.

SafetyDetectives Q2 2020

FLC
FLORIDA LEAGUE OF CITIES

Ransomware... why are we targeted?

- **It works:** Cities, SMB's shown to be willing to pay the ransoms, or extorted to prevent leaked data, encouraging more attacks
- **Valuable Data:** Working and historical data to keep operations going is of great value to both the organization and attackers.
- **Easy to Compromise:** Outdated software/technology, no in-house expertise, lax policies/procedures, tech is increasing in sophistication, budgets are tight, lack of funds for security
- **Remote Work/COVID:** As employees moved out of a secure enterprise network to their home networks, risk of compromise has gone way up

FLC
FLORIDA LEAGUE OF CITIES

Ransomware... why are we targeted?

- **Importance:** Municipalities are more vulnerable not because of the security infrastructure – or lack thereof – but because of the nature of the systems they protect
- **Essential:** DHS identifies 16 critical sectors whose assets are so vital "that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety" – ie. chemical, communications, energy, food and agriculture, healthcare, emergency services, critical dams, transportation, water and wastewater – most of the infrastructure and services that SLG's are responsible for.
- **Better chance$:** A successful attack against vital services like this will have better chances for a payout, ex: Recent hospital attacks.

FLC
FLORIDA LEAGUE OF CITIES

Ransomware... why are we targeted?

You are left with 3 options if you get hit:

- Restore your data from a known good backup
- Start from scratch
- Pay the ransom and hope the attacker gives you the keys to get your data back

FLC
FLORIDA LEAGUE OF CITIES

Ransomware... what if I refuse to pay?

- In 2019, 17.1 percent of U.S. state and local government entities hit paid ransoms vs. 45 percent for all organizations
- Of those that paid, about 60 percent got their data back.
- It has been said that these hackers have better tech support than Microsoft or other software companies

https://www.insurancejournal.com/ 2019

FLC
FLORIDA LEAGUE OF CITIES

Ransomware... what does it cost?

- **Recovery of Costs** (Ransom, forensics, consulting, restoration) In Q1 2019, avg $12,762 increased to $36,295 in Q2, jumped to avg $338,700 by Q4 to $886,625 in 2020. Global costs of ransomware to business were predicted to exceed $11.5 billion annually in 2019 and $20 billion in 2020.
- **Downtime Losses** (5x to 10x the cost of the ransom itself) Downtime due to ransomware attacks average 16 days… or in some cases months or years.
- **Reputation** (Difficult to put a price on your reputation, loss of trust, even losing ability to continue being able to process credit card transactions due to potential PCI violations)

https://www.sungardas.com/en-us/blog/ransomware-attacks-on-us-government-entities/ Q3 2020

FLC
FLORIDA LEAGUE OF CITIES

Breaches... what is the difference?

- **Data Breach –** Any incident where confidential or sensitive information has been accessed without permission. The result of a cyberattack where criminals gain unauthorized access to a computer system or network and steal private, sensitive or confidential personal and financial data of the customers or users contained within.
- **Common cyber attacks used in data breaches:**
  - Ransomware
  - Malware
  - Phishing
  - Denial of Service

https://www.sungardas.com/en-us/blog/ransomware-attacks-on-us-government-entities/ Q3 2020

Breaches... what does it cost?

- **Good news!** Average cost of a data breach has fallen $500,000 compared to last year
  - 100,000 records now costs less than about $3.8M on average (globally)

- **Bad news!** If your organization is located in the US, a data breach costs significantly more.
  - Average cost of a breach in the US is $8.6M – almost 2x global average

https://www.bluefin.com/bluefin-news/key-takeaways-ibm-ponemons-2020-cost-data-breach-report/ Q3 2020

FLC
FLORIDA LEAGUE OF CITIES

Breaches... what does it cost?

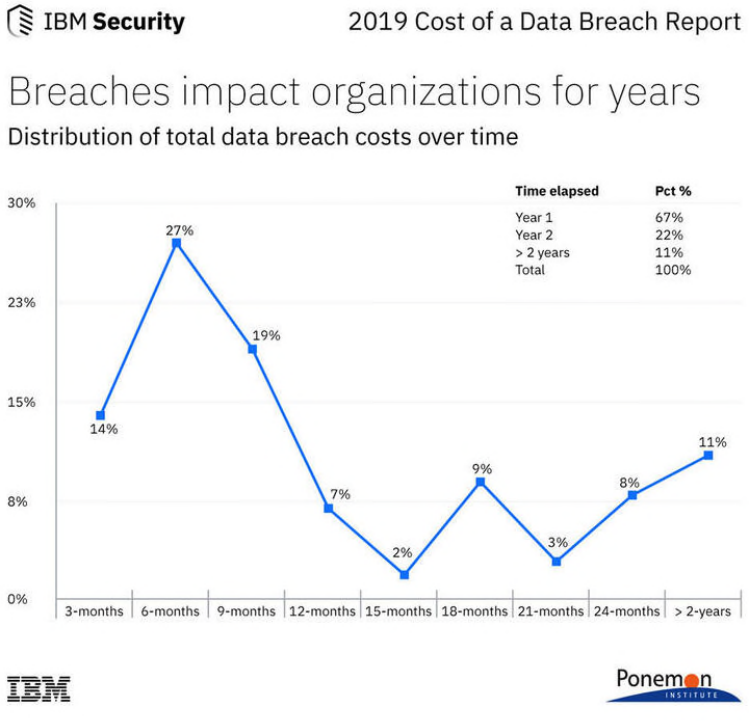
- **Defining what goes into the cost of a data breach**
  - Data breach detection and response
  - Legal fees, fines and settlement costs
  - Cost of victim notification
  - Loss of trust/revenue
  - PR and marketing to regain customer trust
  - Increased support
  - Hidden costs

- **On average, the cost per record is about $150 globally, and $242 in the US**
- **The average breach contains about 25,575 records**

https://www.scasecurity.com/cost-of-a-data-breach Q1 2020

Breaches... what does it cost?

- **Impact over years**
  - **Year 1 = 67%**
  - **Year 2 = 22%**
  - **Year 3 = 11%**



https://www.techrepublic.com/article/how-businesses-can-reduce-the-financial-impact-of-data-breaches/ Q3 2019

FLC
FLORIDA LEAGUE OF CITIES

Breaches... what does it cost?

Response Time Has a Big Impact on the Cost

- On average, it takes 280 days for an organization to discover and contain a data breach – that is almost 1 year!
- If an organization can contain a breach in fewer than 200 days, it saves an average of $1M in losses

Most Costly Industries for a Data Breach

- Healthcare at $7.1 million
- Energy at $6.4 million
- Financial at $5.9 million
- Pharmaceutical at $5.1 million
- Technology at $5 million

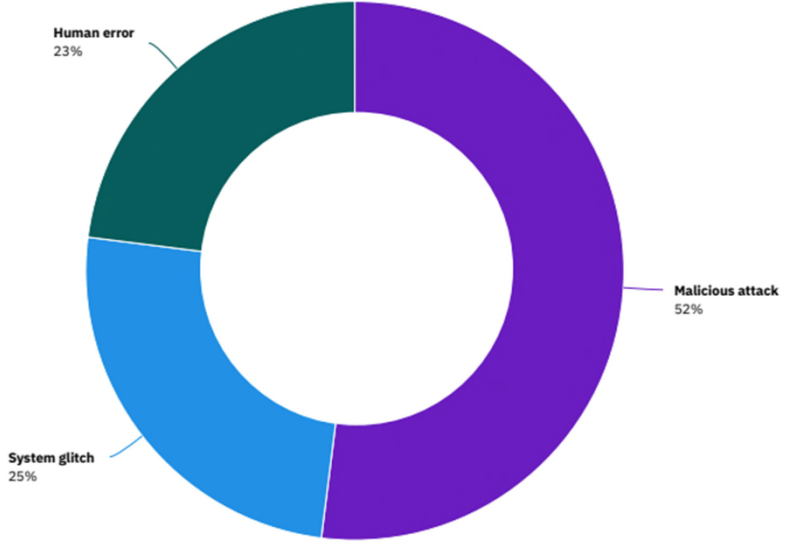
https://www.techrepublic.com/article/how-businesses-can-reduce-the-financial-impact-of-data-breaches/ Q3 2019

Breaches... what does it cost?

Top Causes of a Data Breach

- 52% are the result of a malicious attack
  - 87% of these are criminal gangs, mafia, or others motivated by financial gain
  - 13% are nation-state hackers
- 48% are non-malicious, but no less dangerous
  - 23% caused by human error
  - 25% caused by system glitches

Data breach root cause breakdown in three categories



https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/ Q4 2020

Best Practices... Backups

- Weapons-grade – Image-based backups that are off-line and air-gapped.
- Ransomware is known to attack and encrypt backup sets
- Abide by the 3-2-1 Rule: a minimum of 3 backup copies, using 2 different devices/storage media, with 1 copy off-site.
- Storage media will ultimately fail, so spread risk by using different devices or media… aka redundancy.
- Today's backup solutions can take periodic image backups that replicate to other devices on your network and store data in the cloud. Really, the more backups you have, the better.

FLC
FLORIDA LEAGUE OF CITIES

Best Practices... Patching

- Patches are software updates released on a regular basis to fix bugs or known exploits that hackers or malware commonly use.
- Patches apply to Operating Systems (desktops, servers), appliances, third party applications and hardware.
- Implement a consistent testing and patching schedule
- Utilize a patching application that can distribute and report on deployed patches

Best Practices... Defensive Software

- It is vital to have software in place that filters out the bad from the good before it gets to you.
- A multi-layered approach is necessary:
  - Anti-Virus
  - Anti-Spyware/Malware
  - Email Filtering (ATP)
  - Domain Name Server Filtering
  - Web Filtering

FLC
FLORIDA LEAGUE OF CITIES

Best Practices... Application Whitelisting

- Application Whitelisting software is sophisticated software that defends against ransomware, malware or unwanted software in general.
- Determines if a certain program is on an “allowed” list for permission to run.
- Anything not found on the “allowed” list is denied from running.
- Complex and labor-intensive for IT staff to maintain, but leaves you with an extremely secure and controlled network environment.

FLC
FLORIDA LEAGUE OF CITIES

Best Practices... Employee Training

- General security training should be held on a regular basis to cover rules, general computer security, and dangers found on internet.
- Phishing training should be continuous to test employee's skills at determining if an email is real or fake.
- Implement a security culture where employees are not afraid to ask before they click on a malicious link.
- Special emphasis needed to identify Social Engineering attempts, to identify when hackers are trying to gain access to your network or facilities, or trying to figure out what kind of equipment you're running.

FLC
FLORIDA LEAGUE OF CITIES

Best Practices... Passwords/MFA

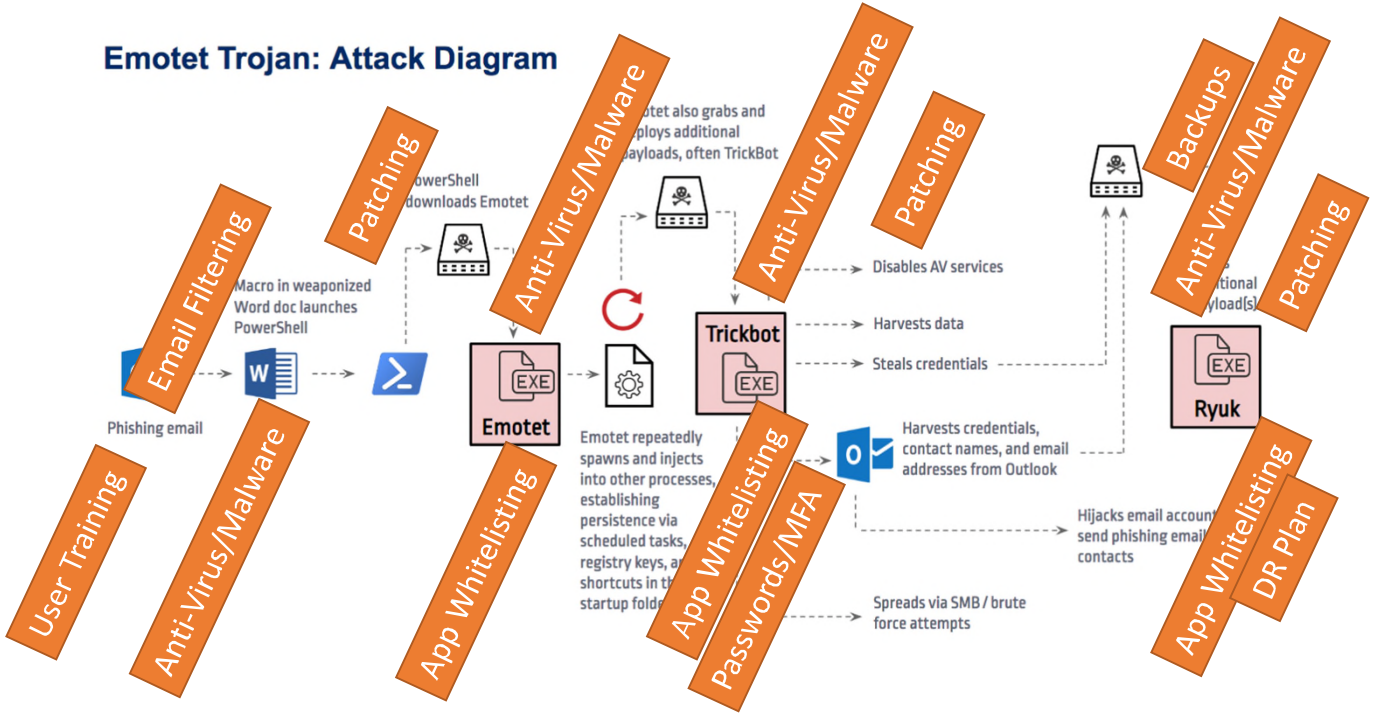
- Passwords alone are no longer considered a secure method to lock down an account.
- Successful phishing campaigns trick employees into giving up their password, allowing an attacker to log in with their credentials, ie. “Account Compromise”
- Utilize Multi-Factor Authentication (MFA) also known as Two-Factor Authentication (2FA), which requires knowledge of 2 pieces of information to log in to an account:
  - The person’s password
  - A random 6-digit code generated each minute
  - In case the password is compromised, the attacker does not have access to the MFA key and cannot log in.

FLC
FLORIDA LEAGUE OF CITIES

Best Practices... Disaster Planning

- Have a plan in place for your organization to recover from an unplanned incident or natural disaster in order to resume normal business operations in a timely manner.
- Continually refine and update as new equipment, personnel or backup methods change or evolve in the organization.
- Update your plan at least 1x per year at a minimum.

Ransomware... how does it work?



FLC
FLORIDA LEAGUE OF CITIES

Questions... you should ask today!

1. Do we have backups that absolutely cannot be touched by ransomware?
2. Has this been independently verified?
3. Do we allow direct Remote Desktop Protocol connections?
4. Have we had a recent network assessment/penetration test?
5. Do we have a Security Awareness Training program?
6. Does our firewall provide internet filtering along with intrusion prevention/detection?
7. Do we have a solution for installing updates for ALL systems?
8. What IoT devices do we have and how do we secure them?
9. Do we have cyber insurance? What does it cover?
10. How do we verify our 3rd parties and other partners have adequate security?

FLC/FLGISA's Leading Role…

- Extremely popular Cybersecurity/Ransomware panel workshop at FLC Annual Conference
- Ransomware and other similar hot topics led by FBI and vendors were a huge success at FLGISA Annual Conference.
- Cyber Security Roundtables regularly featured through the FLGISA
- Series of 4 Ransomware webinars held in short succession trained over 1820 local government officials and employees across FL
- Cybersecurity Best Practices article being featured in last Fall 2019-2020 Quality Cities magazine
- Partnership with Cyber Florida/USF, holding 4 regional cyber workshop for executives and elected officials – Cyber Security War Game!
- Coordination with FLGISA, FCCMA, FACC, etc. as well as FMIT and FACT for continued Best Practices training for our membership
- Working on potential Cybersecurity Funding program nationally and through State of FL
- NEW: Developed a program through an FMIT Safety Grant to encourage cities to start using secure Cloud backups in order to minimize risks of being held hostage by ransomware.

FLC
FLORIDA LEAGUE OF CITIES

Some Takeaways…

- Data breaches are simply a fact of life
- It's not a matter of IF… it's a matter of WHEN
- Cybersecurity expenditures reduces risk of a breach

Resources…

- Your friendly IT Department! ☺
- MS-ISAC (Multi-State Information Sharing & Analysis Center)
- DHS/CISA (Cybersecurity & Infrastructure Security Agency)
- Cyber Florida
- FLGISA (Florida Local Government Information Systems Association)
- Florida League of Cities – mvanzwieten@flcities.com


QUESTIONS?

Thank you!

FLGISA
FLORIDA LOCAL GOVERNMENT INFORMATION SYSTEMS ASSOCIATION

Michael J. van Zwieten, CGCIO, MCSE
Director of Technology Services, Florida League of Cities
Executive Director, FLGISA
407-367-1794
mvanzwieten@flcities.com

FLC
FLORIDA LEAGUE OF CITIES