HOW DIGITAL FORENSICS CAN PLAY A ROLE IN DEFENDING YOU, YOUR COMPANY AND YOUR EMPLOYEES

Participants:

Santiago Ayala (ATX Forensics)

Aaron Weiss (Forensic Recovery)

ATX FORENSICS LLC

Forensic Recovery

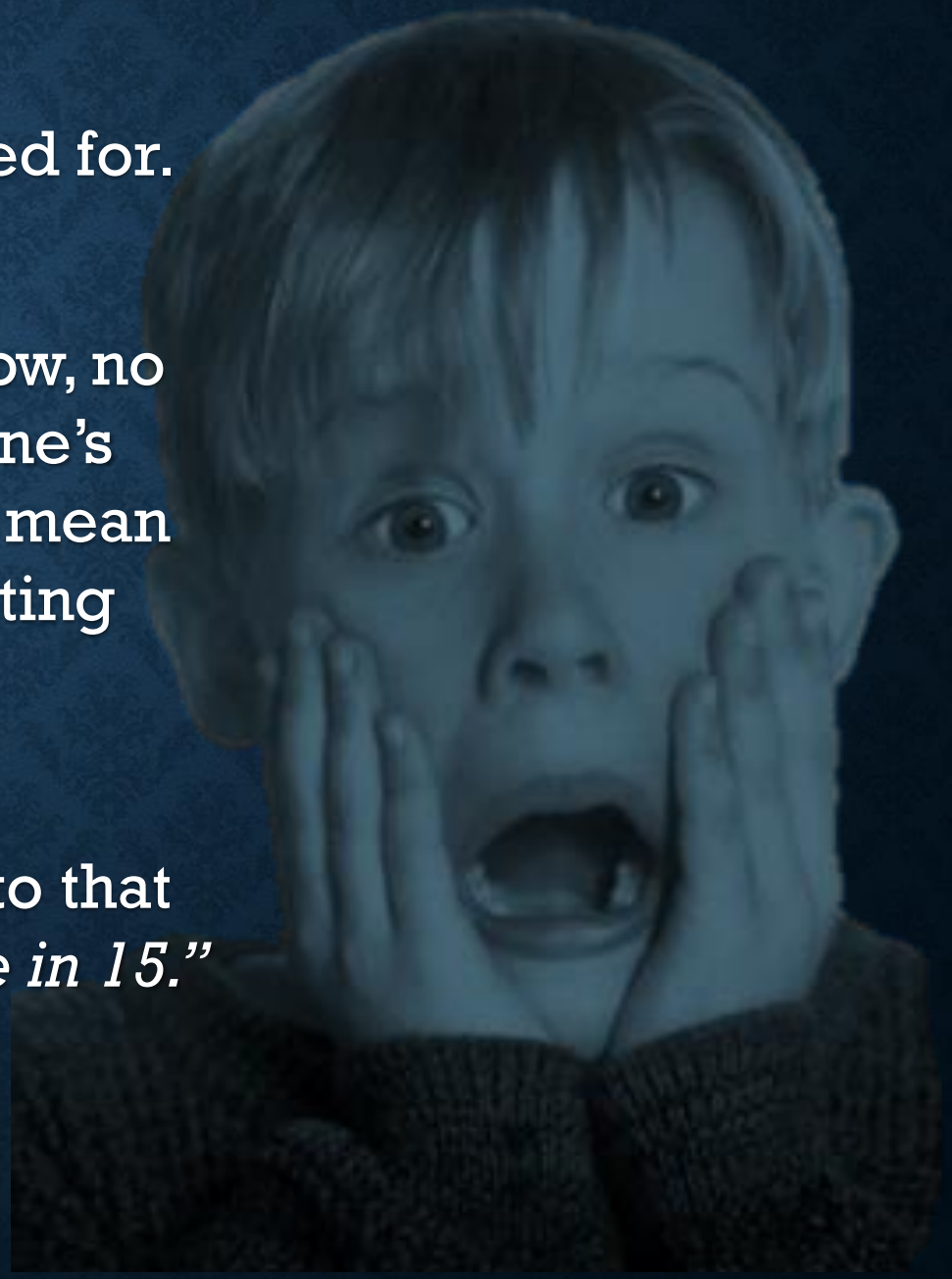
Digital Evidence Recovery Solutions

MONDAY MORNING ON YOUR DRIVE IN, YOU RECEIVE THAT TEXT:

Something you weren't expecting… or prepared for.

With no plan in place, no response plan to follow, no in-house digital investigator to lean on, everyone's looking at you to call the next shot. This could mean job security or means you're going to be updating your resume very soon.

We're here today to make sure your response to that text is : *"Hold tight. We have a plan. I'll be there in 15."*



AGENDA

- Have a plan
  - Policies and Procedures
  - Legal
  - Response plan
- Don’t spoil it (the evidence, that is)
- In case you need an example
- Best practices for safeguarding data

PREPARATION

- Policies – What you do
- Procedures – How you do it
- Incident Response Plan - Practice it!
- Legal Authority
  - Monitor communications
  - Collect digital evidence from both work and personal devices used for business (BYOD; Veriato/Spector360)
- Acceptable Use Policy

DEVELOP INCIDENT RESPONSE PLAN

- Who is the lead? Are you the lead? CISO? President?
- Who needs to be notified and are there timelines for notification?
  - IT Security (to maintain log files or triage incident)
  - IT Support (so they do NOT affect investigation)
  - Legal, Compliance, and/or Executives
  - HR
  - Public Relations
  - Law Enforcement
  - Employees (in the case of a phishing attack or social engineering threat)

DEVELOP INCIDENT RESPONSE PLAN

- Evidence Preservation Plan
  - Identify priorities
  - Internal resources or third-party expert?
  - Continue to monitor employee or intruder activity?
  - Preserve existing security logs
  - Do we need to isolate systems, take them off-line, or disconnect network connections?

DON'T SPOIL THE EVIDENCE

We're going to get to some case examples, and as we're going through them, we want you to be keeping in mind the opportunities where someone could be inadvertently destroying evidence that could be viable to our investigation.

FORENSIC INVESTIGATION

Basis Steps

- Don't step on the evidence
- Collection / Preservation
- Analysis
- Report

Q: What happened?

Most logging systems have a finite amount of activity they record (usually limited to storage space or a time frame)… just like a DVR security system. We are losing evidence by letting these logs roll over, so we need to notify the right personnel to make sure they extend the storage capabilities or make backups of the current and future logs while the investigation is ongoing.

It is very typical for persons **to inadvertently destroy** much-needed evidence in an attempt to eradicate a threat. When one detects a virus, our first instinct is to get rid of it… possibly by **restoring a computer** to its factory settings. By doing so, we erase traces to its source and we are unable to learn how it is operating.

Tasking unqualified persons to preserve and collect evidence can render that evidence inadmissible in court.

If a key employee or suspect employee is terminated, handing their computer over to their replacement without preserving can overwrite evidence of wrongdoing… which is often discovered many months later.

It also makes it difficult or impossible to point the finger at the right person!

CASE 1 – INTERNATIONAL CASE OF BRIBERY AND CORRUPTION

- Large corporation in the manufacturing industry
- Identification, what trigger the suspicion?
- Who identified the potential matter?
- Interviews
- Monitoring (what tools can be utilize? who should be involved? …)
- Language barriers
- BYOD policies (Can you install monitoring software on BYOD?)
- Social Media / Chat

CASE 2 – CORPORATE ESPIONAGE

- You receive a tip that a key employee is leaving to start his own company
- Refer to plan and notify the right people
- Monitor activity and have the legal right? (i.e. Spector 360, appliance)
- Should we make a forensic copy of the device?
- Does this person have the capability to delete files, restrict access (i.e. are they IT Admin, Executive)?
- If being terminated, coordinate with IT so that access is revoked while being terminated (including remote access and mobile device access).

CASE 3 – HACKING / BREACH

- Unauthorized third- party has gained access to your company's crown jewels.
- Who discovered the incident?
- What triggered the discovery?
- Execute the plan…but wait, do we have a plan?

  (Cue the Audience participation)

SOME BEST PRACTICES

We can all do to reduce the risk of a compromise

STOP AND THINK

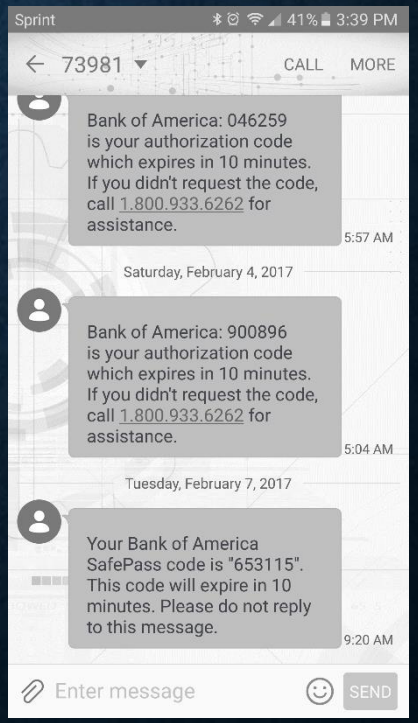
- What kind of data am I the custodian of?
- Am I storing this data in a safe location?
- Who else can access this file?
- What happens if an unauthorized person receives this email?
- Is my password easy to access or guess?
- Did I think about what happens to this data when I press SAVE/SEND?

LEAST PRIVILEGE / NEED TO KNOW

- Access controls
- Expire File Share links
- Revoke access when an employee/personnel is terminated or no longer on project
- Give privileges at the lowest level NEEDED
  (i.e. no admin accounts)

TWO-FACTOR AUTHENTICATION (2FA)

- Requires two of the following:
  - Something you HAVE, ARE, or KNOW
- Can be a physical key, app, or text message or fingerprint

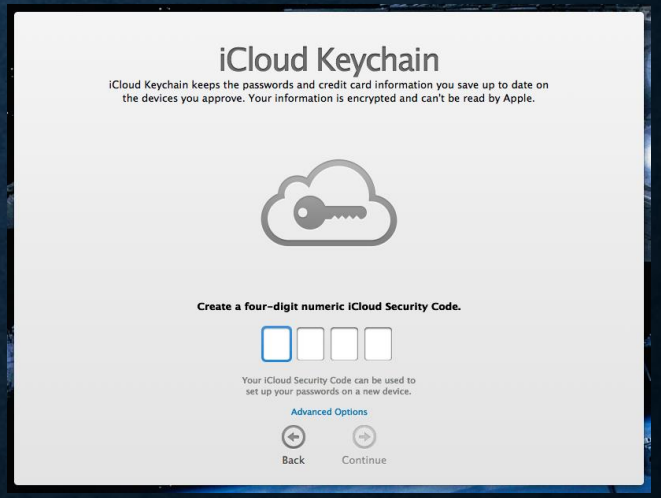


STRONG AND UNIQUE PASSWORDS

- Use a password manager that can generate strong, unique passwords for website, accounts and applications
- Can be used in browsers, mobile devices, and enterprise
- Should implement also use 2FA for access

LastPass •••|

KeePass
Password Safe

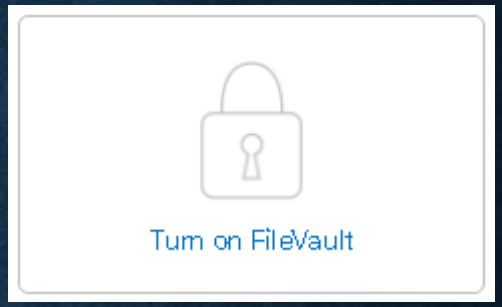


PORTABLE DEVICES

- One of the BIGGEST RISKS!!!
- Consider if your smartphone, tablet or laptop was lost or stolen
- Can you track it?
- Can you wipe it?
  - Many mobile devices /accounts (iOS, Android, Windows) have the capability to locate and remotely wipe a device if lost or stolen

FULL DISK ENCRYPTION

- Is your device encrypted?



- Many are free. Compare them:
  https://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software

REMOTE EMPLOYEE

- Employee is working from home…
- Is his business network segregated from home network?
- Using separate work-only computer?
- Is he going to use his own mobile device?
  - If so, can you remotely wipe your data from his device?

REMOTE ACCESS

- Configure alerts for remote access anomalies
  - Geographical
  - After hours
  - Failed passwords
- Use Mobile Device Management (MDM)
- Virtual Private Network (VPN); Remote Desktop
- Configure Windows login auditing
- Maintain firewall and operating system logs for at least 1 year.

Thanks!

Santiago Ayala (ATX Forensics)

Twiter: @atxforensics, @darthsaac | info@atxforensics.com

Aaron Weiss (Forensic Recovery)

aweiss@forensicrecovery.com

ATX FORENSICS LLC

Forensic Recovery

Digital Evidence Recovery Solutions