FORENSIC INVESTIGATION

of Insider Threats

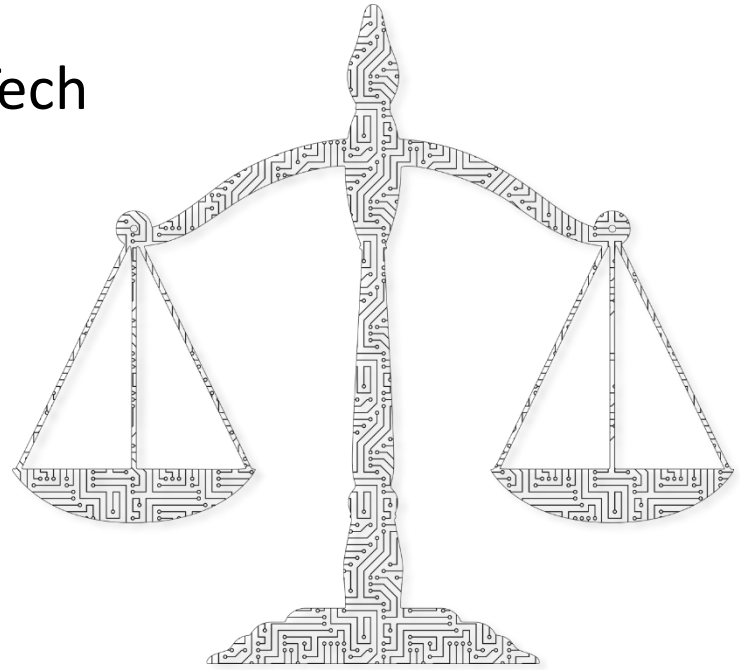
ABOUT

① Digital Forensics Unit (DFU) Examiner at INA

② Training Instructor at Exterro

③ Former Missouri State Public Defender (MSPD) Digital Forensics Examiner

④ Former BDO Forensic Tech



AGENDA

① Insider Threats

② Characteristics of At-Risk Businesses

③ Best Practices

④ Case Studies

⑤ Q & A

DEFINE: insider threat

The inherent risk of harm that an individual with access to an organization's assets poses.

① May act alone or in a group

② Could be a current or former employee, contractor, or partner

③ Both intentional and unintentional

FACTS - insider threats:

① Incidents of insider threats have doubled since 2018

② The majority of incidents are caused by negligence

③ Privilege abuse takes the longest to discover

CHARACTERISTICS of at-risk businesses

① Too much trust is placed in employees

② No backup employees

③ Universal passwords for all devices

④ Security policies not followed

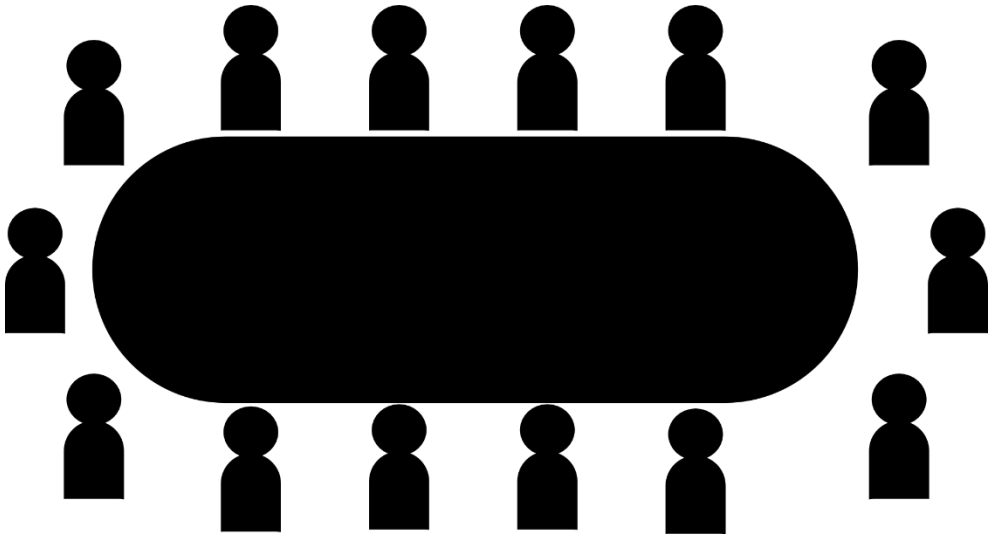
CHARACTERISTICS of at-risk businesses: leadership

① Not tech savvy

② Does not prioritize IT

③ Possess administrative credentials

④ Does not enforce policies



CHARACTERISTICS of at-risk businesses: IT personnel

① May not exist

② Transitioning roles/New

③ Doing the job of 3+ people

④ Lacking resources and cooperation

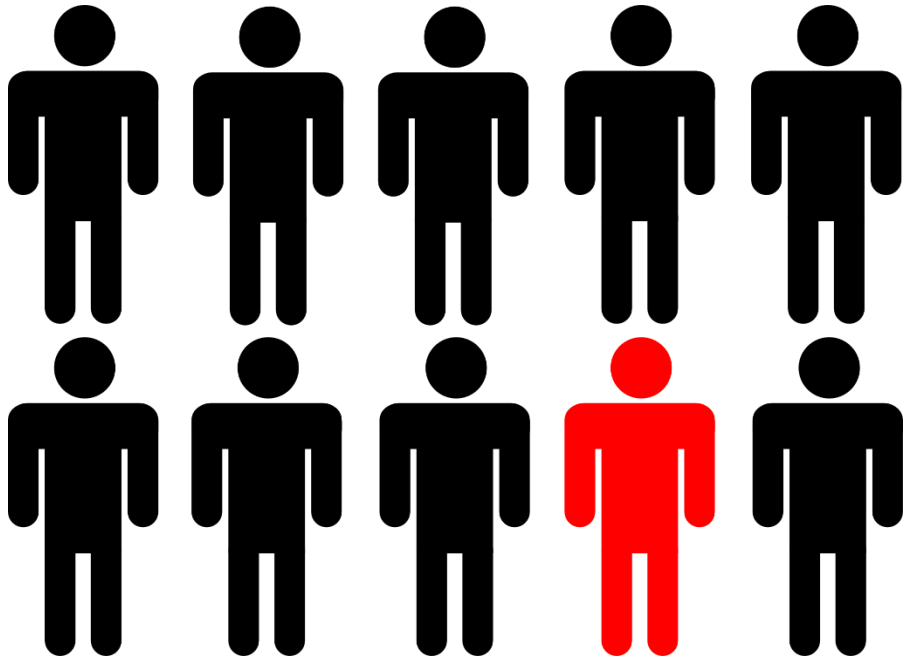
RED flags

① Working late and never taking vacations

② Defensive

③ Attempts to sidestep or violate policies

④ Data hoarding/downloading



WE can be friends

① IT Departments are essential to forensic investigations

② An independent, unbiased third party will ensure objectivity

③ IT personnel and forensic examiners can work as a team

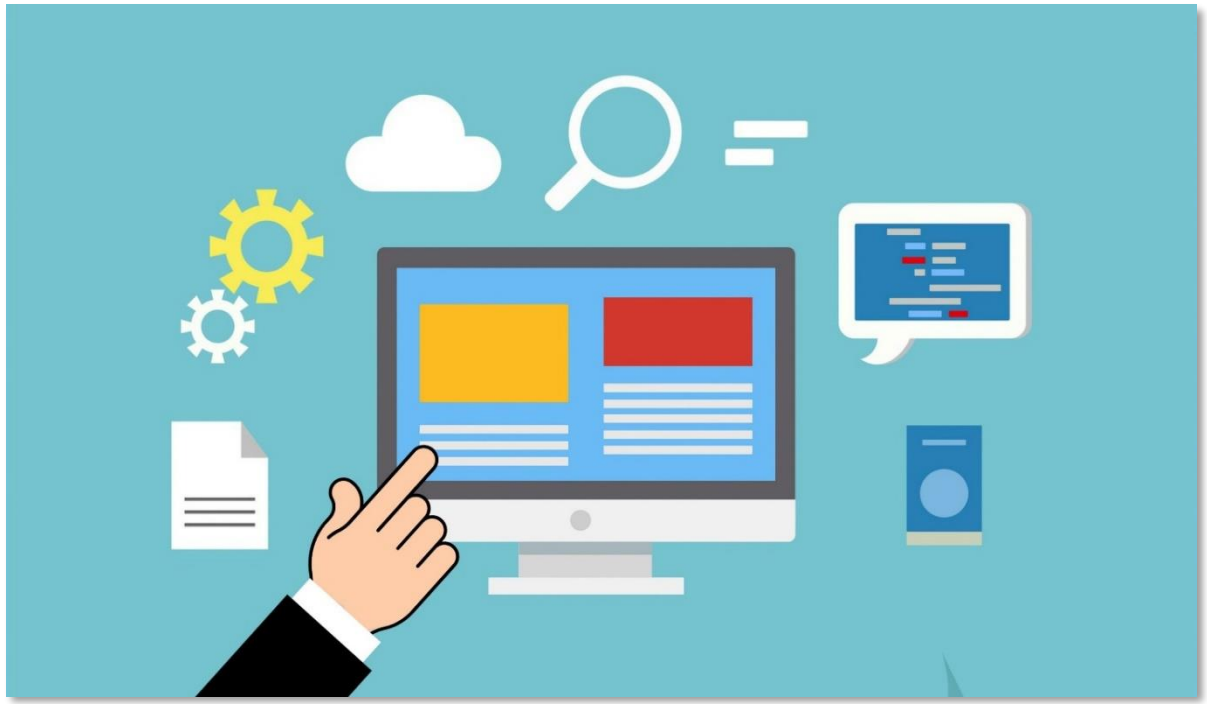
BEST practice

① Turn on logs and extend the retention periods

② Image computers of departing employees

③ Limit privileged access

④ Restrict or block USB ports



COLLECTION

① Isolate device from network or disable access

② Do not access; could alter data

③ Provide necessary details to forensic examiner

④ Be aware data could be time-sensitive

Case study

Bad Bookkeeper

BAD bookkeeper

① Recently acquired agricultural business

② No backups for office employees

③ Bookkeeper rarely took time off

④ Bookkeeper resisted involving accountants

BAD bookkeeper

① INA DFU performed after-hours onsite collection

② The evidence was staged, processed, and analyzed

③ Objective - export QuickBooks files and perform further analysis

④ Password recovery techniques were employed on the files

BAD bookkeeper

What were the signs of insider threats?

What could have been done differently?

Case study

BEC Stands for Big Executive Catastrophe?

BEC stands for big executive catastrophe?

① Busy staffing company used IT vendor

② No password policies or multi-factor authentication in place

③ President was not tech savvy

④ Regularly sent check to collaborating company

BEC stands for big executive catastrophe?

① Received email notification asking for wire transfer

② Wired over $150,000 to account provided

③ INA DFU examined mailbox and O365 logs

④ Less than 20% of theft was recovered

BEC stands for big executive catastrophe?

What were the signs of insider threats?

What could have been done differently?

Case study

Very Problematic VP

VERY problematic vp

① VP of engineering firm frequently worked late

② Held administrative credentials

③ Resigned with little notice

④ President hired INA DFU to examine computer

VERY problematic vp

① Began analysis looking for evidence of exfiltration

② Located and recovered deleted PST

③ Mailbox examination yielded side business communication

④ User activity analysis showed file transfers to USB

VERY problematic vp

① Located side business invoices in Chrome cache

② Further analysis revealed actual unauthorized engineering work

③ Findings resulted in court order for personal devices

④ Additional evidence located; case still in litigation

VERY problematic vp

What were the signs of insider threats?

What could have been done differently?

Case study

Uncivil Civil Servant

UNCIVIL civil servant

① Large school district with security division

② Security head’s number seen on state bid portal

③ INA DFU was hired to examine devices

④ Objective - investigate and determine extent of violations

UNCIVIL civil servant

① Examined iPhone and computer

② Knowledge of alleged actions limited

③ Substantial amount of communication data present on phone

④ Keyword searches and database examinations were unsuccessful

UNCIVIL civil servant

① Digging into contacts and voicemails identified involved parties

② Voicemail from accountant produced light bulb moment

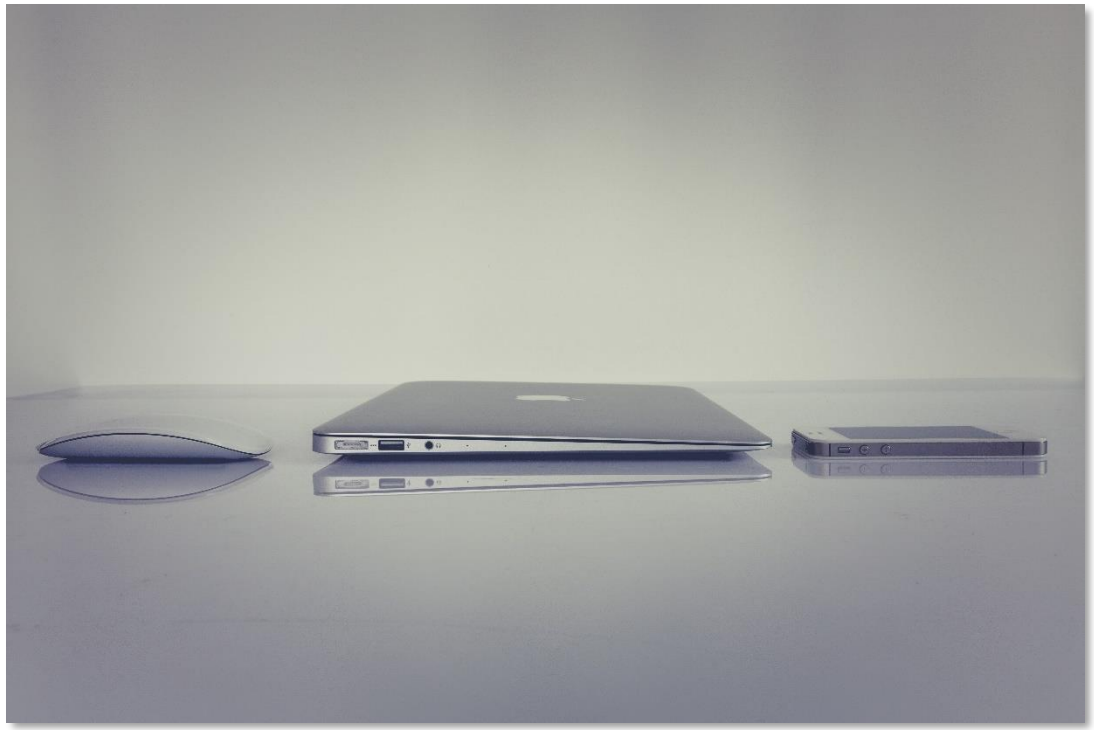
③ Searched and located communication with parties of interest

④ Findings resulted in termination and revoked pension

UNCIVIL civil servant

What were the signs of insider threats?

What could have been done differently?



THANK you!

Kate Davenport, EnCE, CCPA, ACE
INA Digital Forensics Unit
kdavenport@ina-inc.com
717-562-7774 (direct)