WELCOME TO THE 11TH ANNUAL HACKING CONFERENCE

The Institute of Internal Auditors
Chicago

ISACA
Chicago Chapter

WELCOME TO THE 11TH ANNUAL HACKING CONFERENCE

Check-In Code: sweepleg

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

TALES FROM FORENSIC INVESTIGATIONS

AGENDA

INTRODUCTION

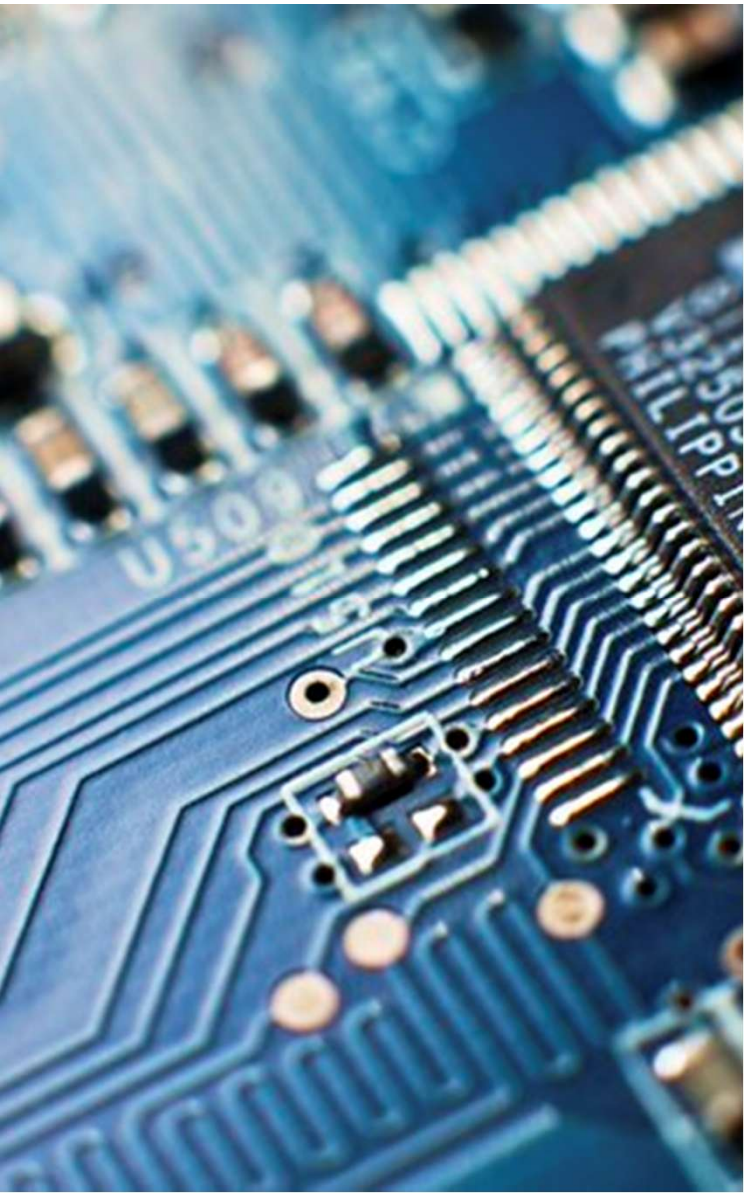
FORENSICS OVERVIEW

FORENSIC TALES

FOUR GOALS OF AN INVESTIGATION

DIY VS OUTSIDE HELP

PREVENTION TIPS

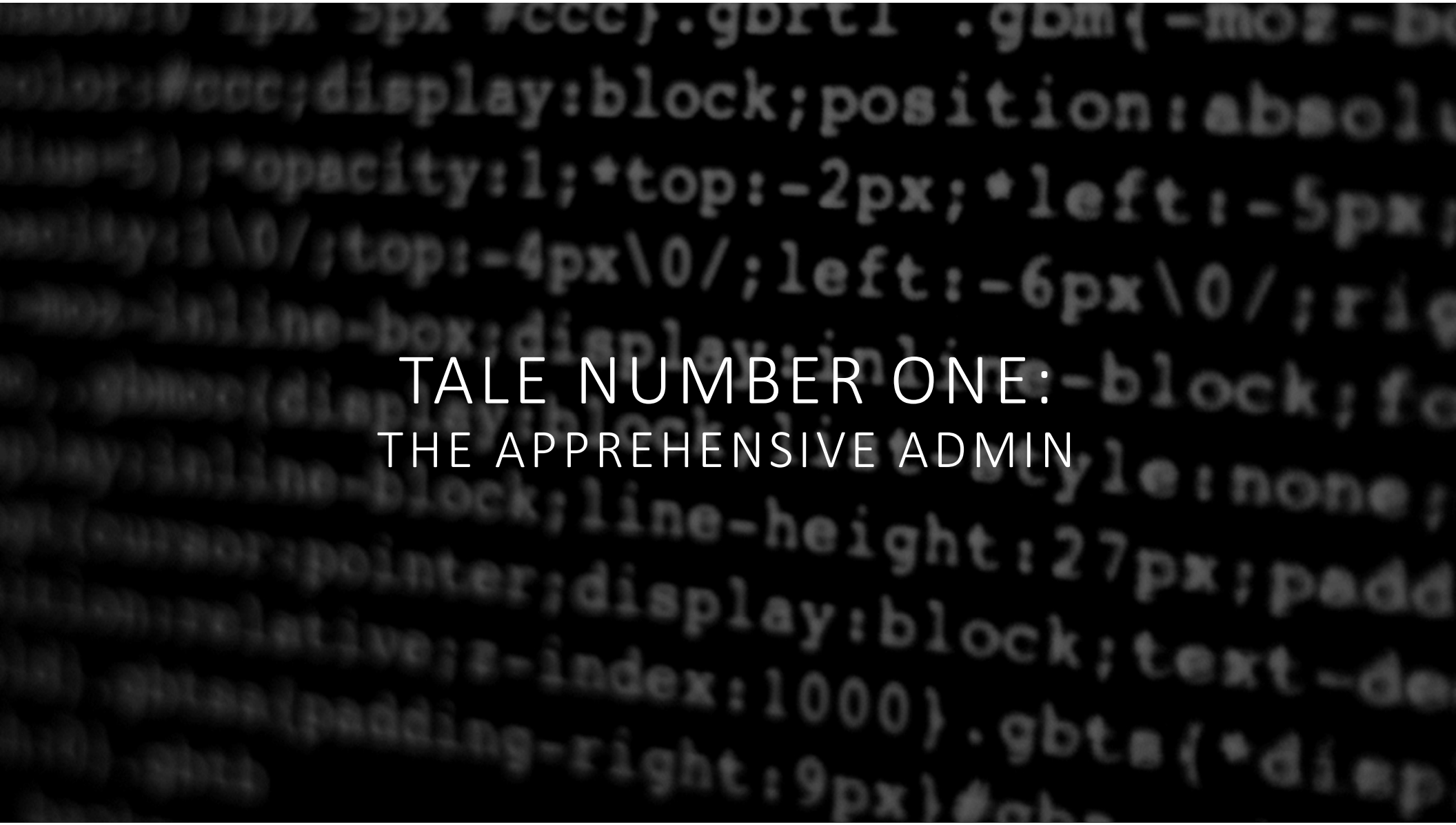


STU DEKEN

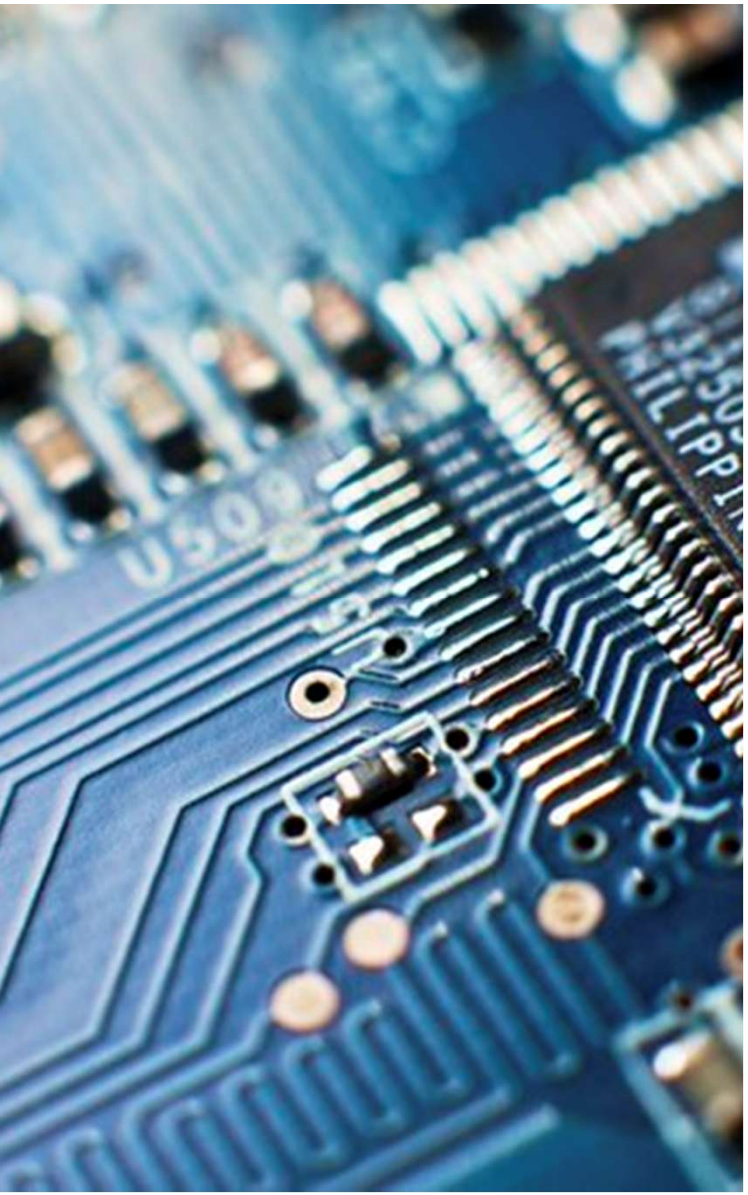
- Digital Investigations Manager, RubinBrown
- Former police officer
- Computer crimes task force
- Expert witness testimony
- Litigation support, fraud investigations, misconduct, email and system compromise

FORENSICS OVERVIEW

INVESTIGATION FOUNDATION

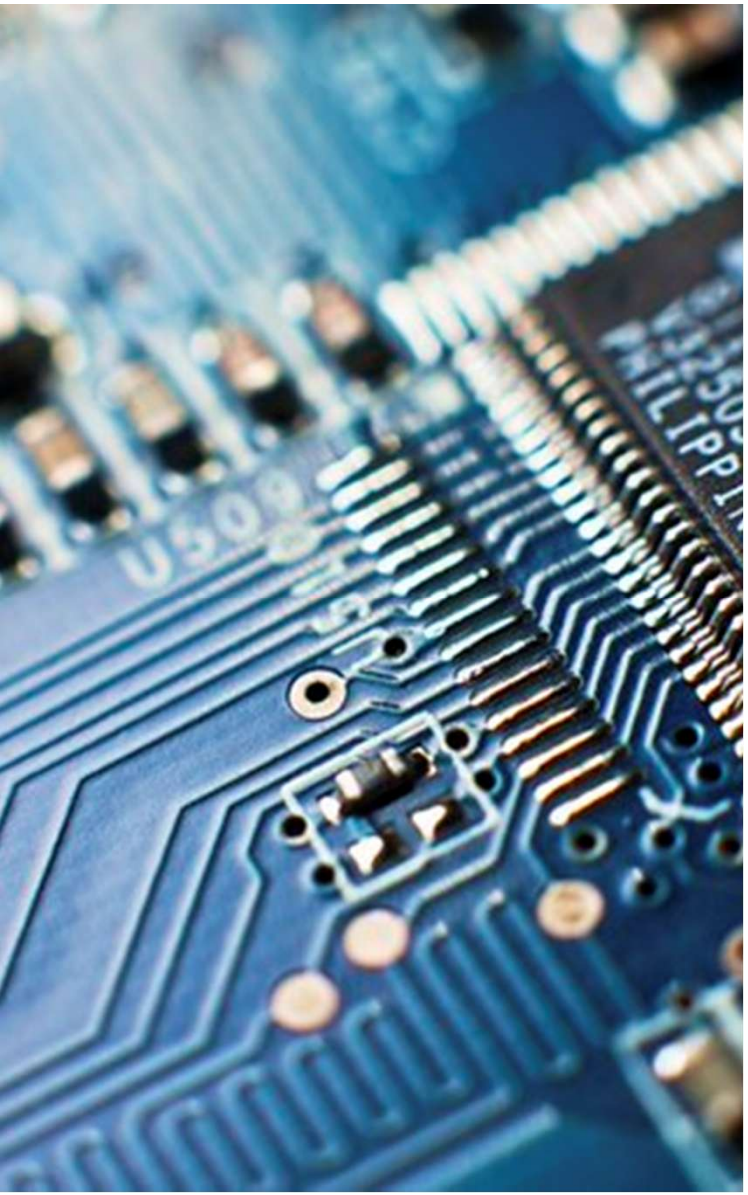


TALE NUMBER ONE:
THE APPREHENSIVE ADMIN



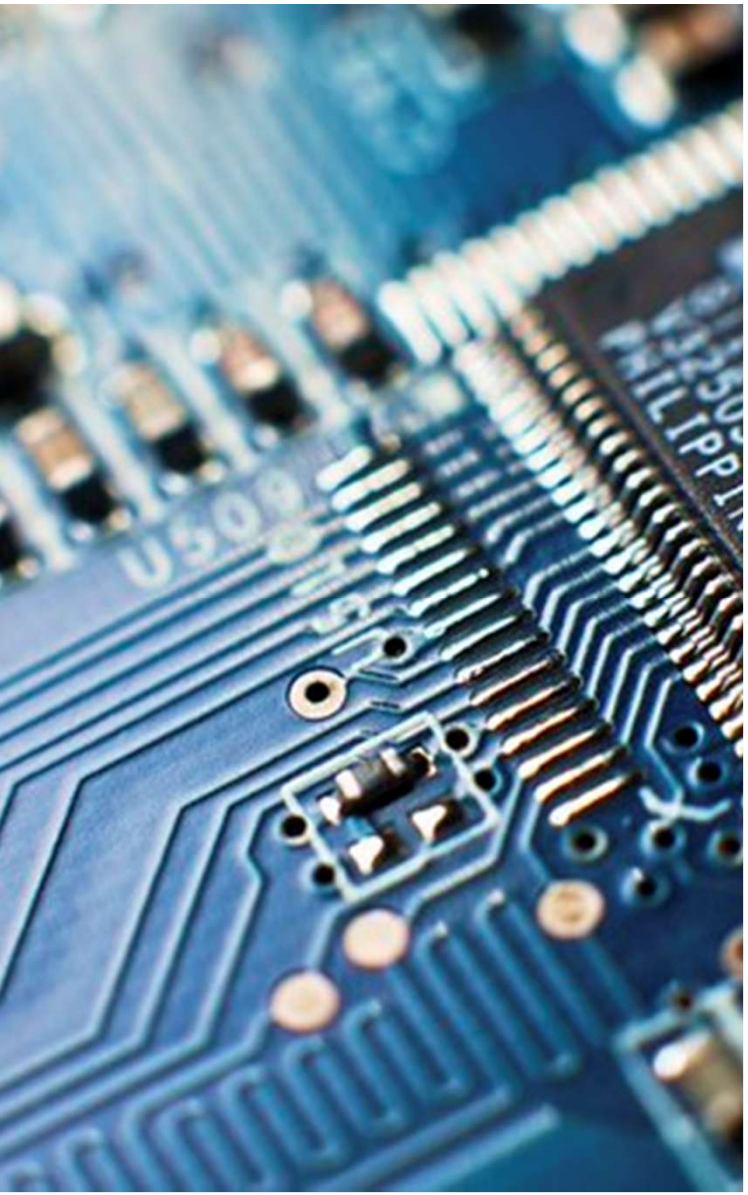
THE APPREHENSIVE ADMIN

- Leadership of a local nonprofit organization was worried one of their Exchange Administrators was reading sensitive emails to/from members of the leadership team.
- They contacted us, seeking confirmation.
- We initiated a forensic investigation.



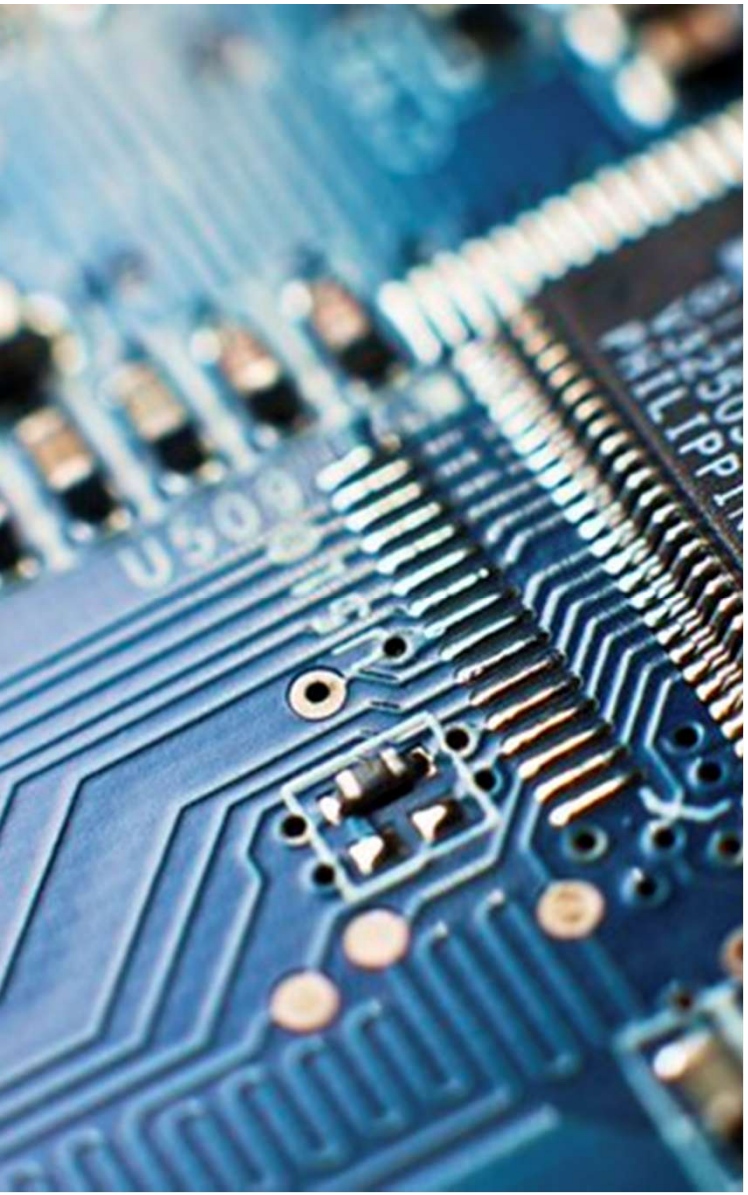
FORENSIC TIDBIT

- Microsoft logs actions in the Microsoft365 environment via the Unified Audit Log.
- These actions include logins, emails sent, emails deleted or moved, documents accessed in Sharepoint, etc.
- One of the logs that is captured is called “Folderbind” which indicates that a user accessed a specific mailbox (theirs or someone else’s).



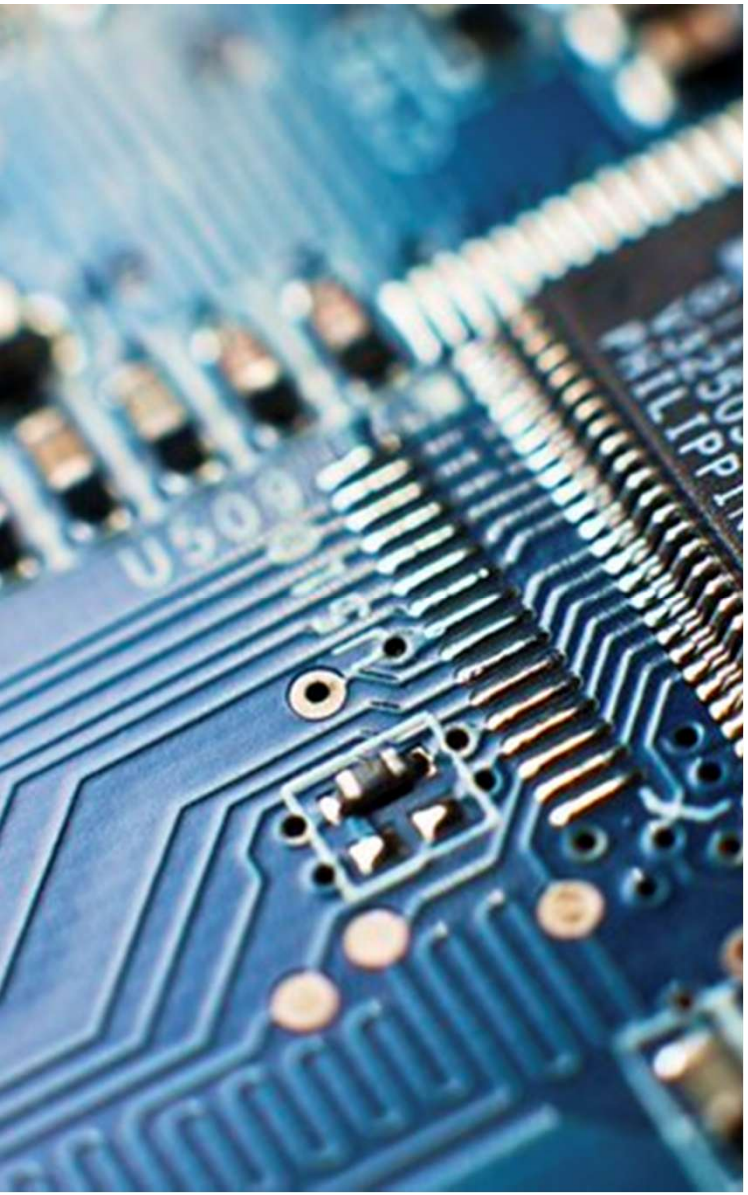
INVESTIGATION QUESTIONS

- Are there any “Folderbind” logs between the subject of the investigation and other users, specifically members of leadership?
- What days and times did it occur? Could it line up with work-related duties?
- Did any of the other Exchange Administrators have similar activity?
- Can we determine anything else about the suspect’s activities?



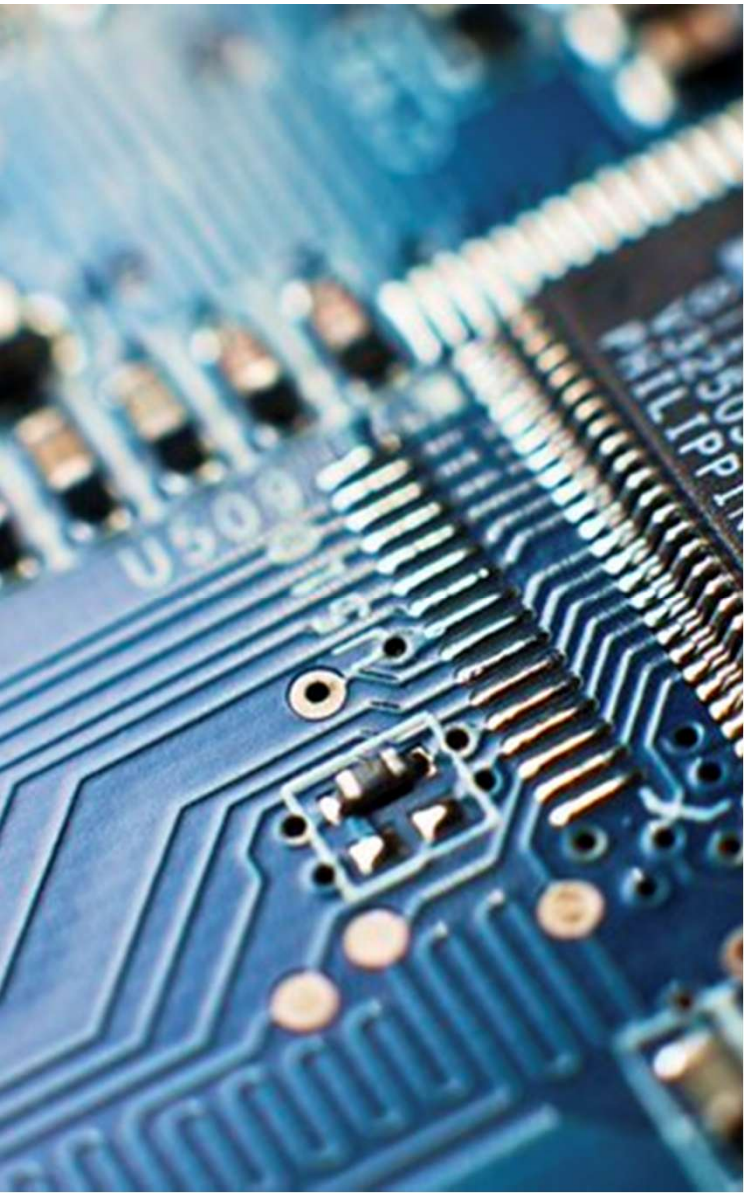
INVESTIGATION RESULTS

- The suspect did have numerous “Folderbind” actions to mailboxes, largely contained to the leadership
- Days and times were widely varied and included weekends, holidays, and late night/off work hours.
- No one else had similar activity.
- We were able to demonstrate some specific messages accessed via the “Update” log.



AFTERMATH

- Why didn’t the in-place alerts to the IT team catch this?
- How can it be prevented in the future?

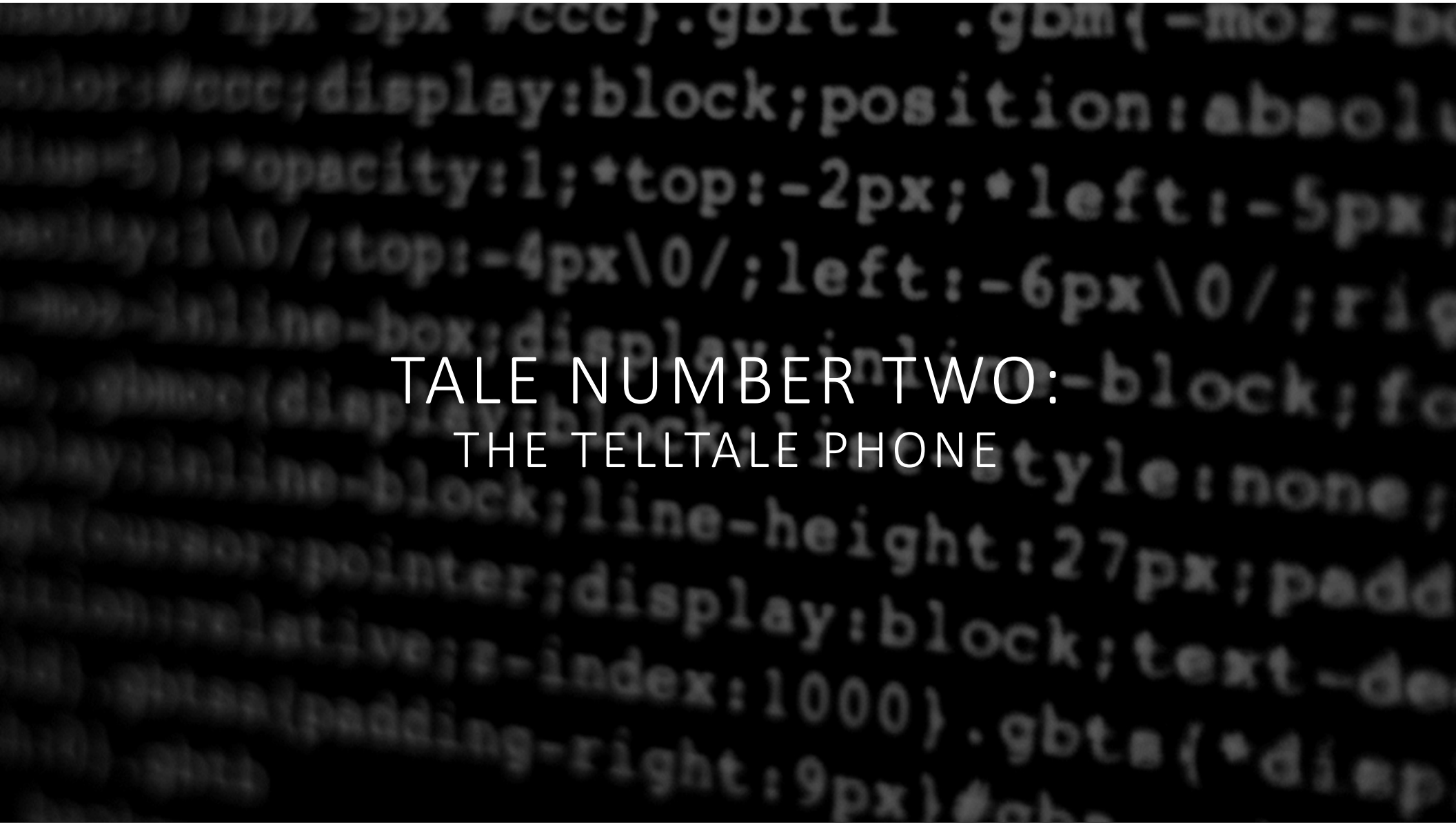


LESSONS LEARNED

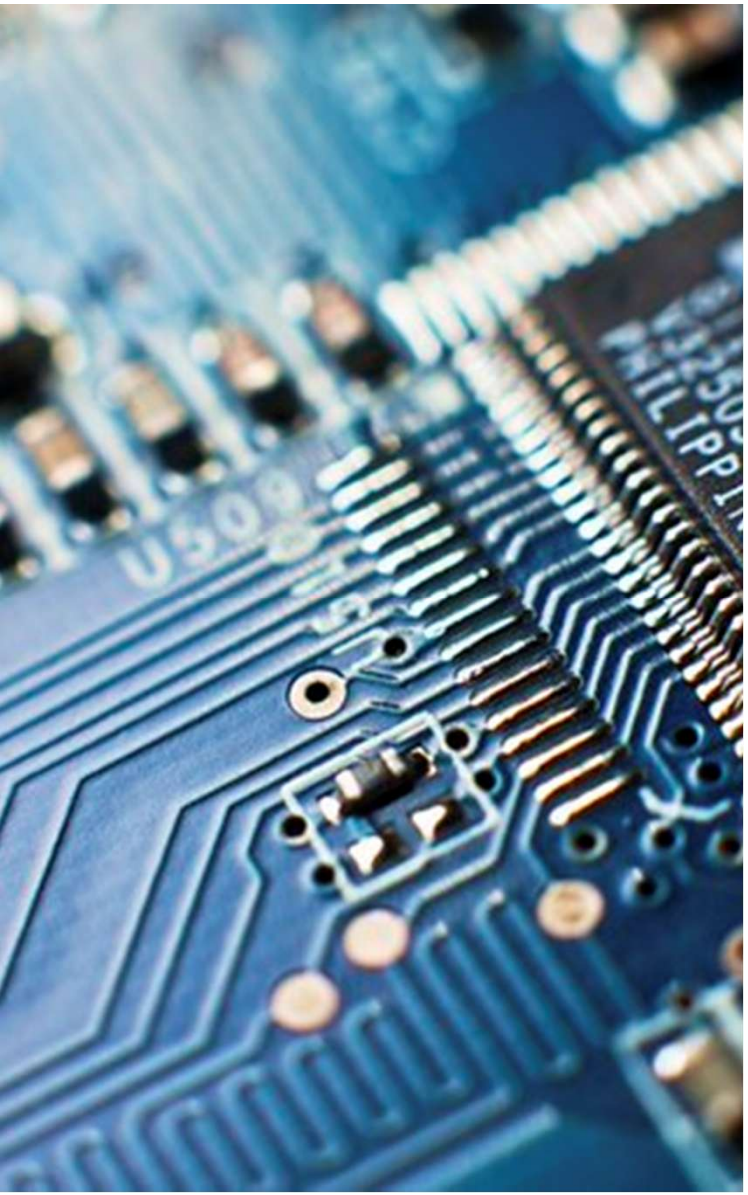
- Most digital activity is going to leave traces
- Even knowledgeable people often can’t avoid leaving evidence
- Trusted members still need oversight
- Never assume that processes work- testing is critical

POLLING QUESTION ONE

HAVE YOU HAD AN INCIDENT THAT REQUIRED A FORENSIC INVESTIGATION IN THE LAST YEAR?

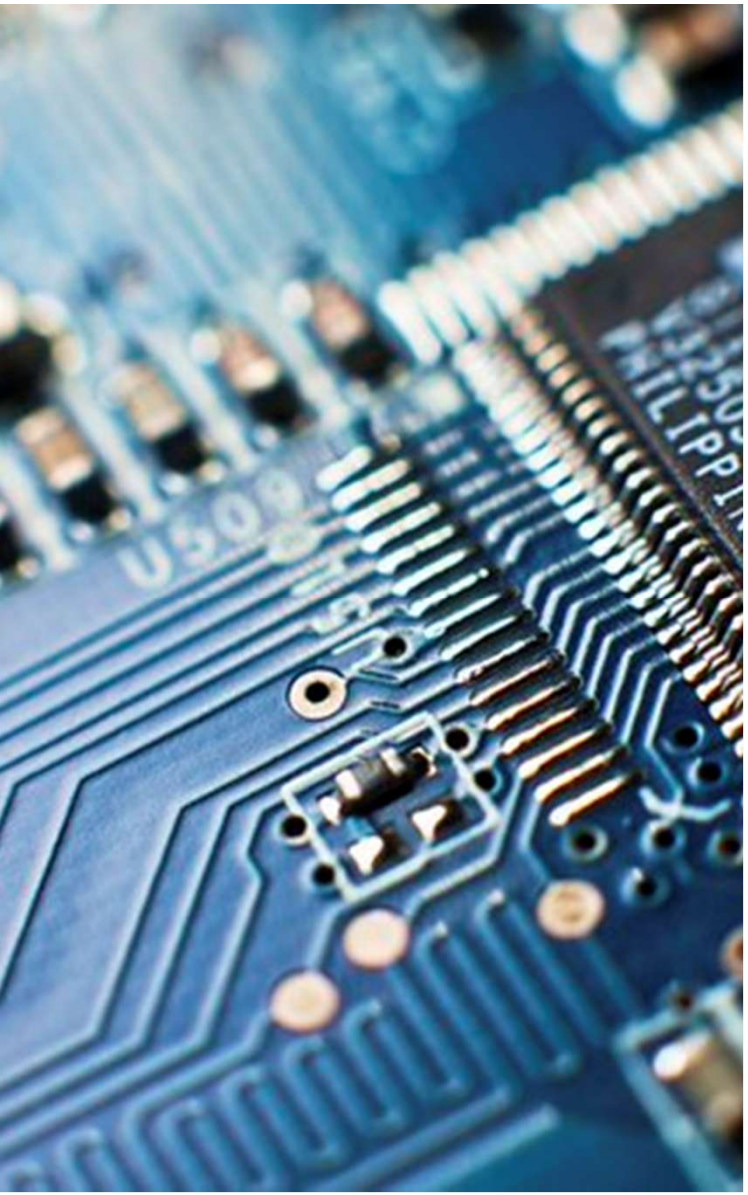


TALE NUMBER TWO:
THE TELLTALE PHONE



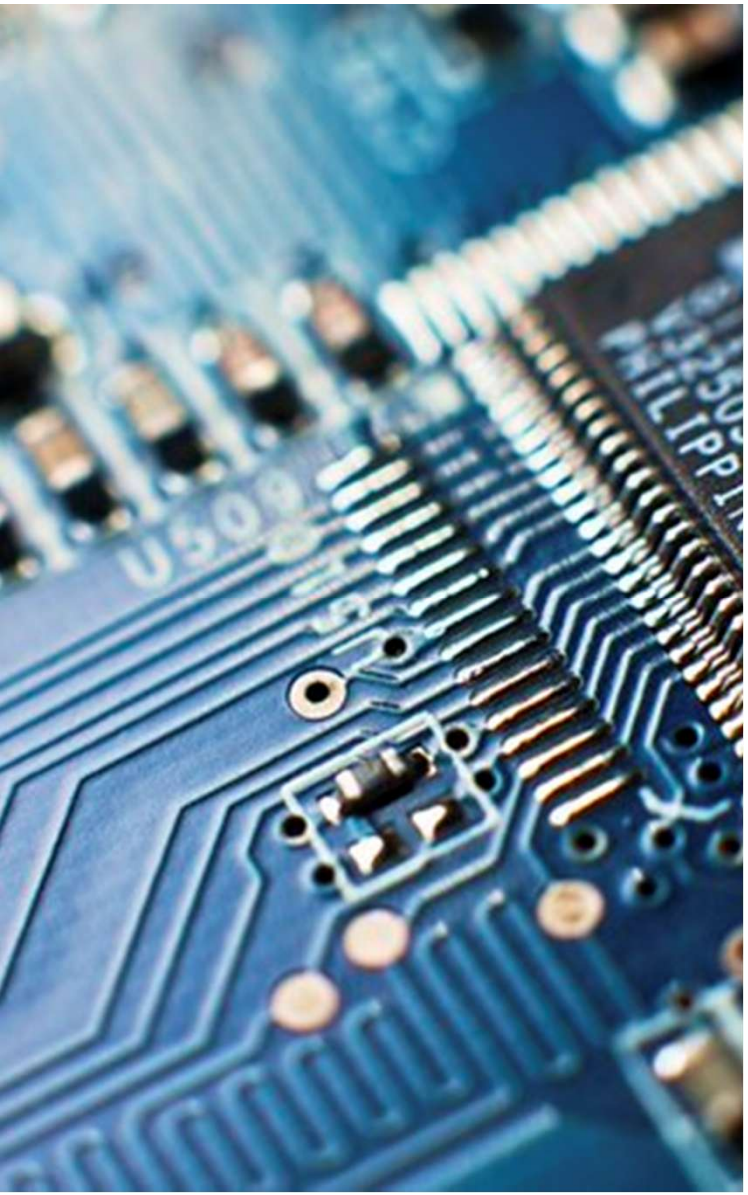
THE TELLTALE PHONE

- A local café/convenience store was burglarized.
- The suspect stole cash, lottery tickets, and other valuable merchandise, and then set a fire to cover their tracks.
- The video system survived the fire and provided the first bit of evidence.
- The primary investigators needed assistance identifying and confirming a suspect.



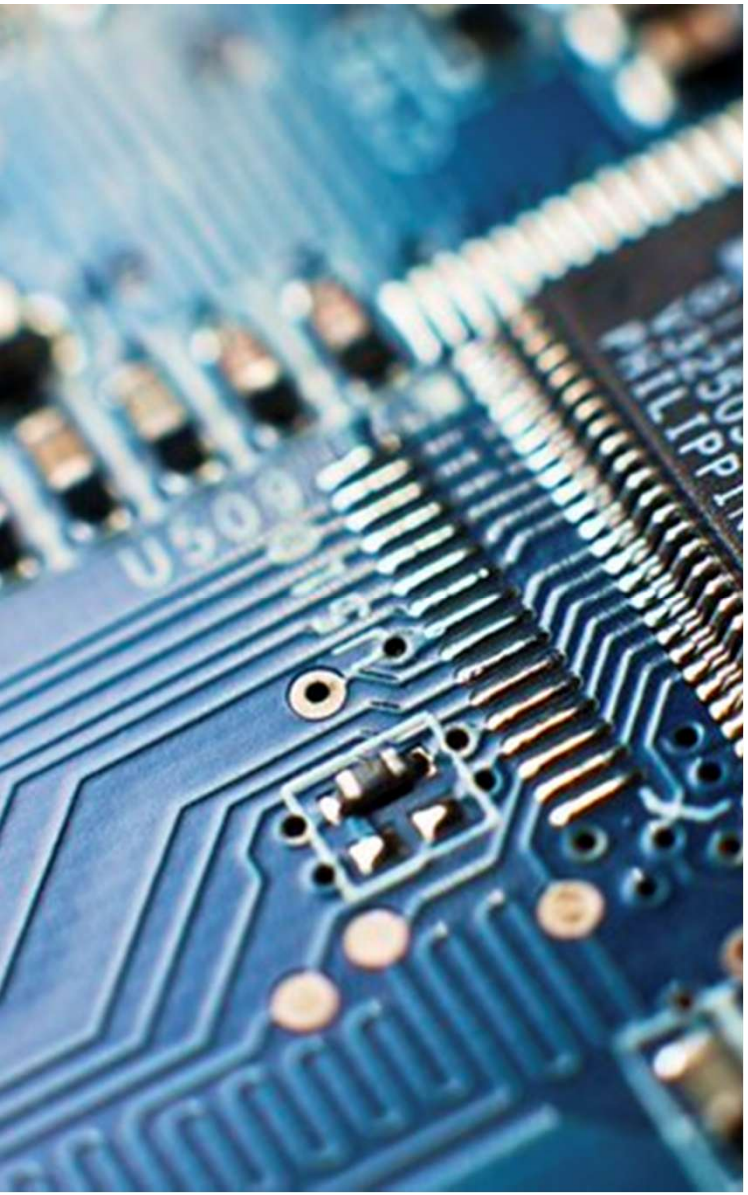
FORENSIC TIDBIT

- Modern Cell Phones contain a *ridiculous* amount of data about us.
- This can include location data, email and internet searches, app use, etc.
- One of the things that your phone captures is a list of networks and devices you connected to.



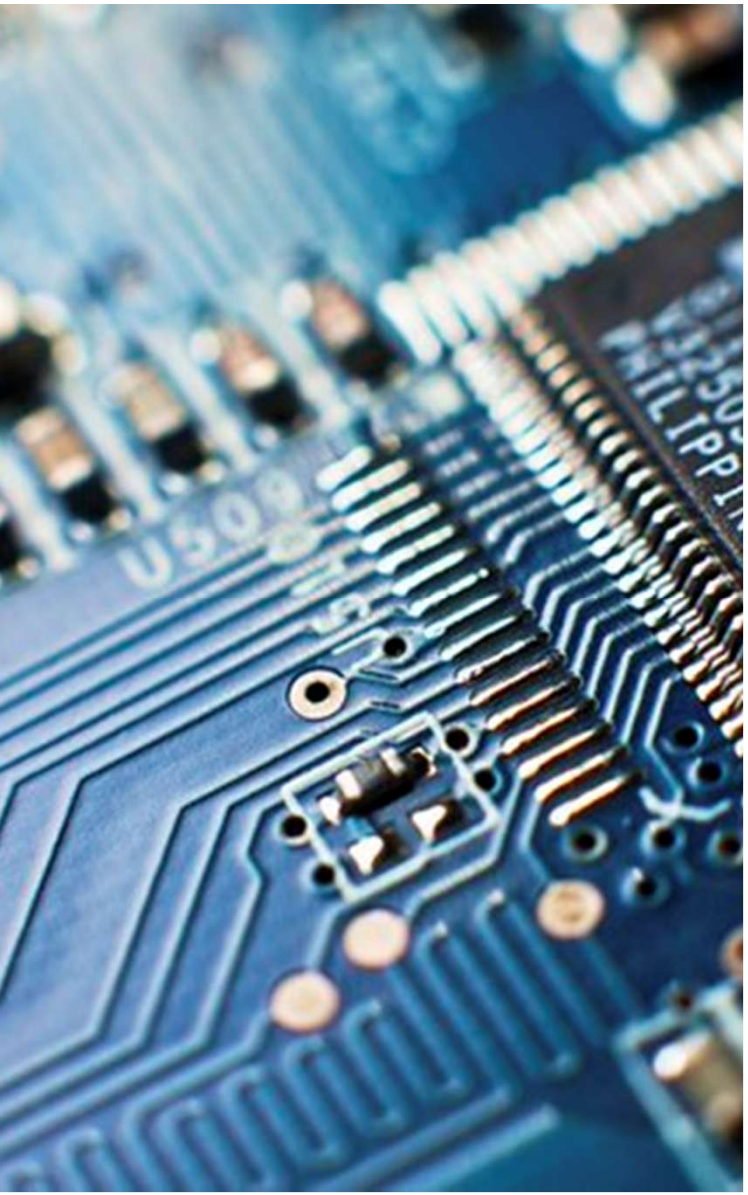
INVESTIGATION QUESTIONS

- Can we tie a potential suspect to the scene at the time of the crime?
- Can we say with certainty it was them?
- Were they alone or with others?



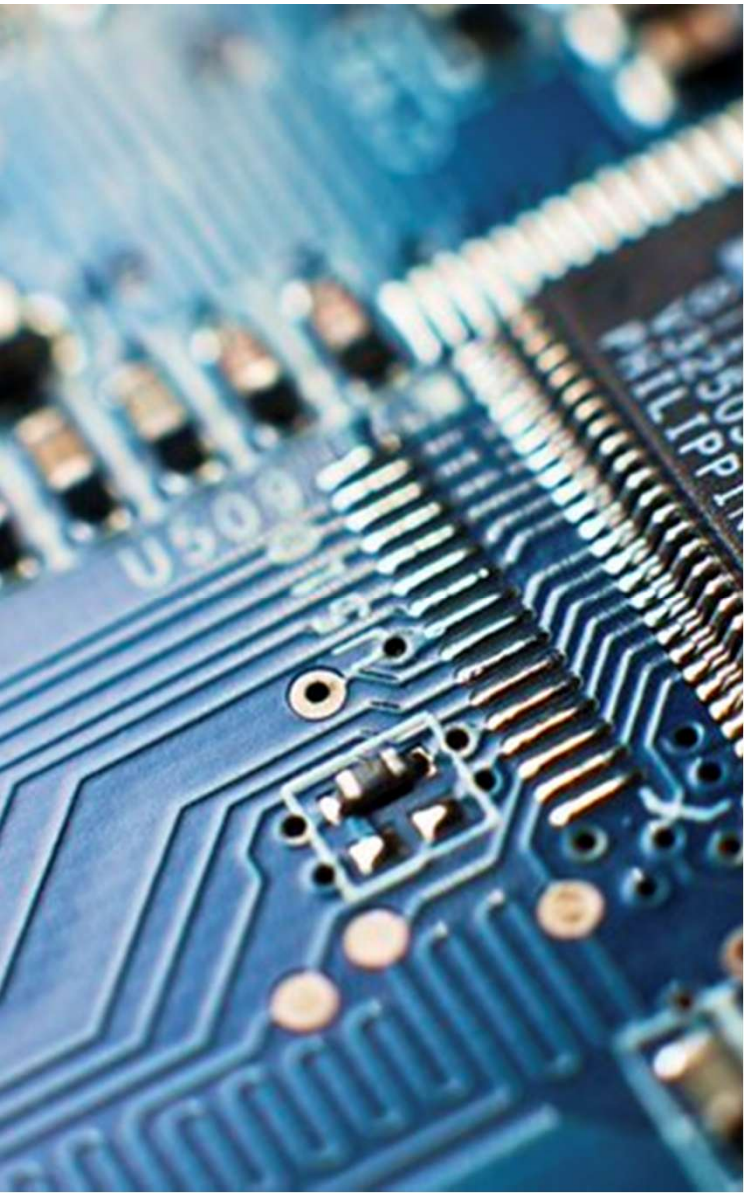
INVESTIGATION RESULTS

- The suspect's phone connected to the wifi less than a minute before the break-in occurred and no other devices connected for several hours on either side of the event.
- This was confirmed first via the wifi router and later by an analysis of the suspect's phone.



AFTERMATH

- Confession and later plea bargain
- Wider training point for all area departments

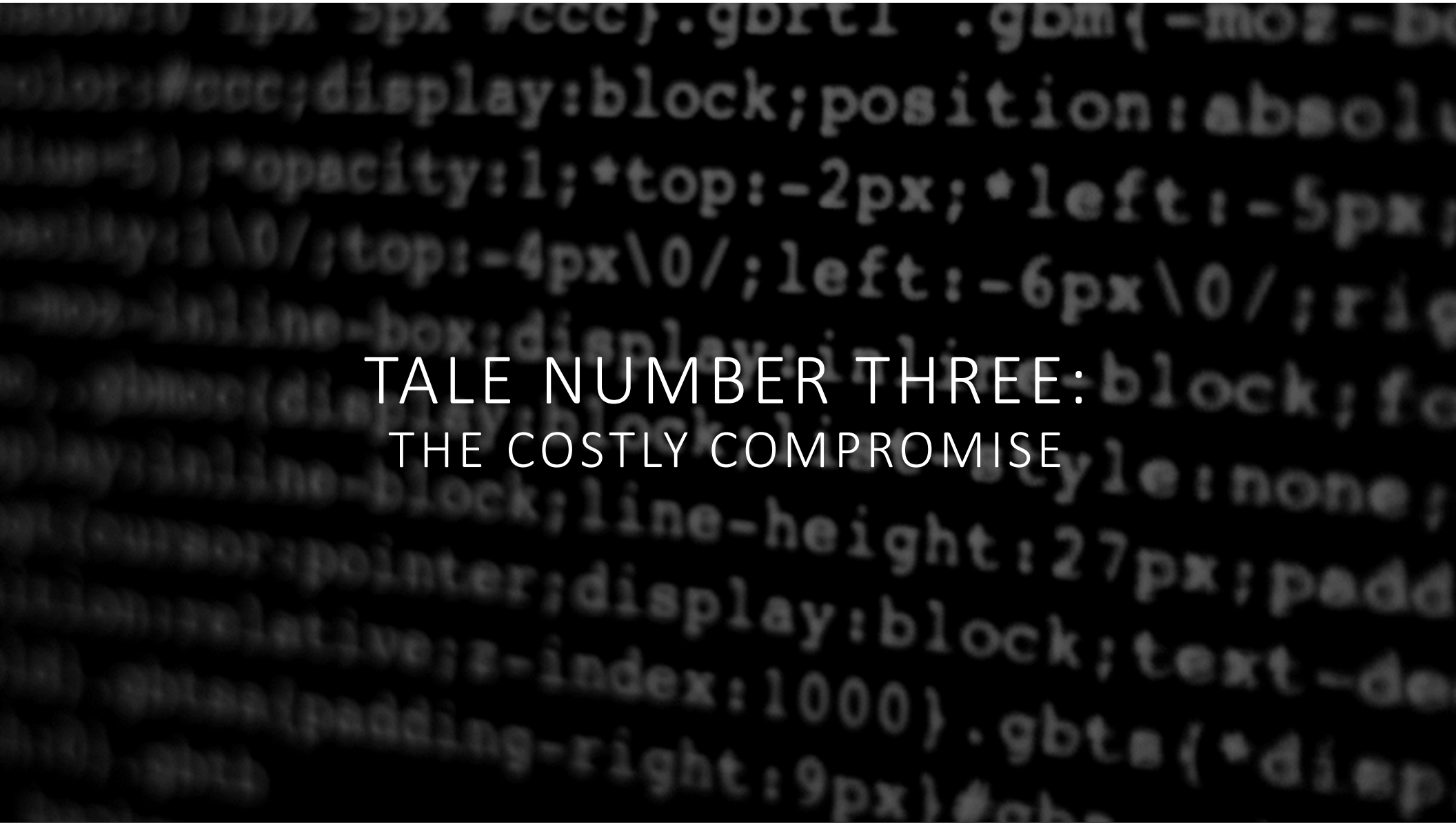


LESSONS LEARNED

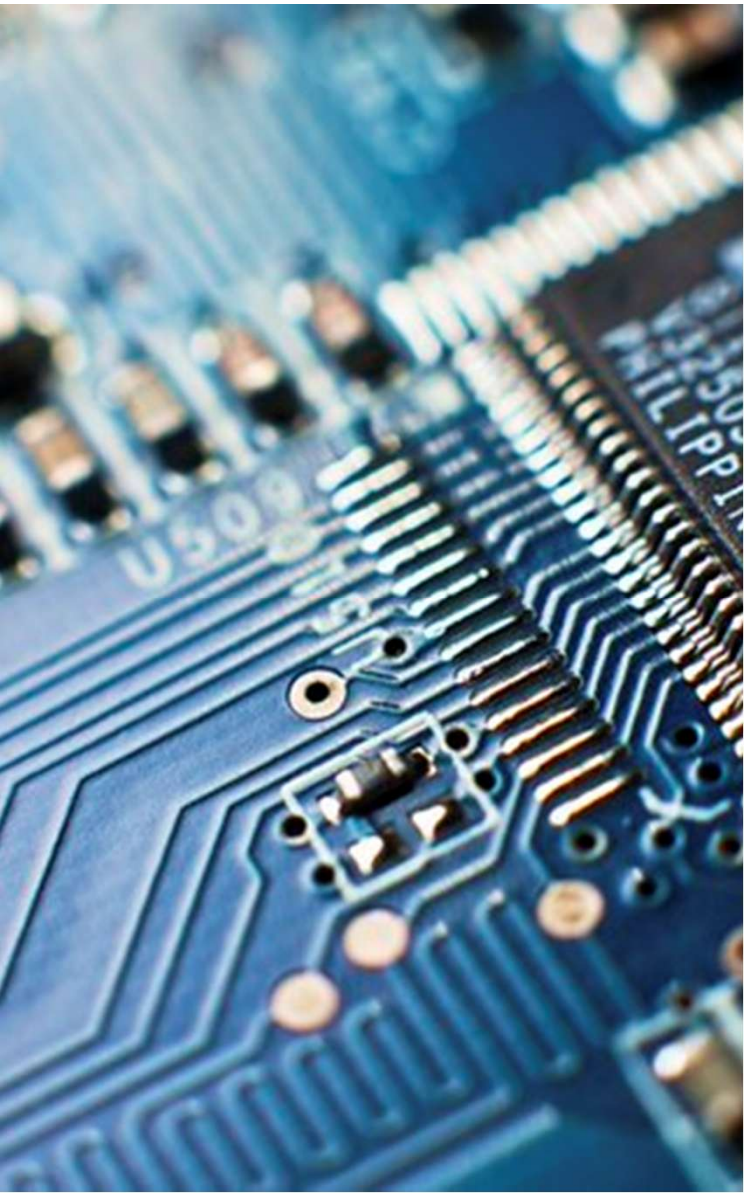
- Fast action is critical
- There are often electronic traces even in incidents that aren't "cybercrimes"
- Cooperation is critical

POLLING QUESTION TWO

HAVE YOU IDENTIFIED POTENTIAL VENDORS FOR FORENSIC SERVICES?

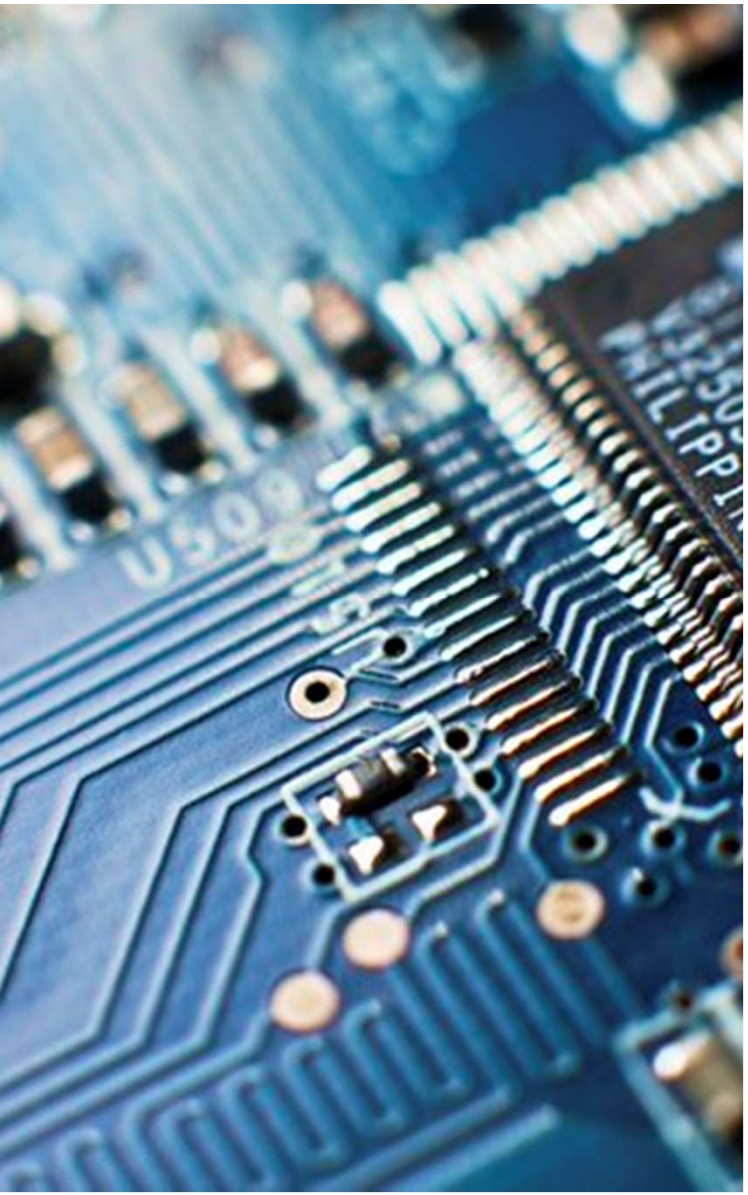


TALE NUMBER THREE:
THE COSTLY COMPROMISE



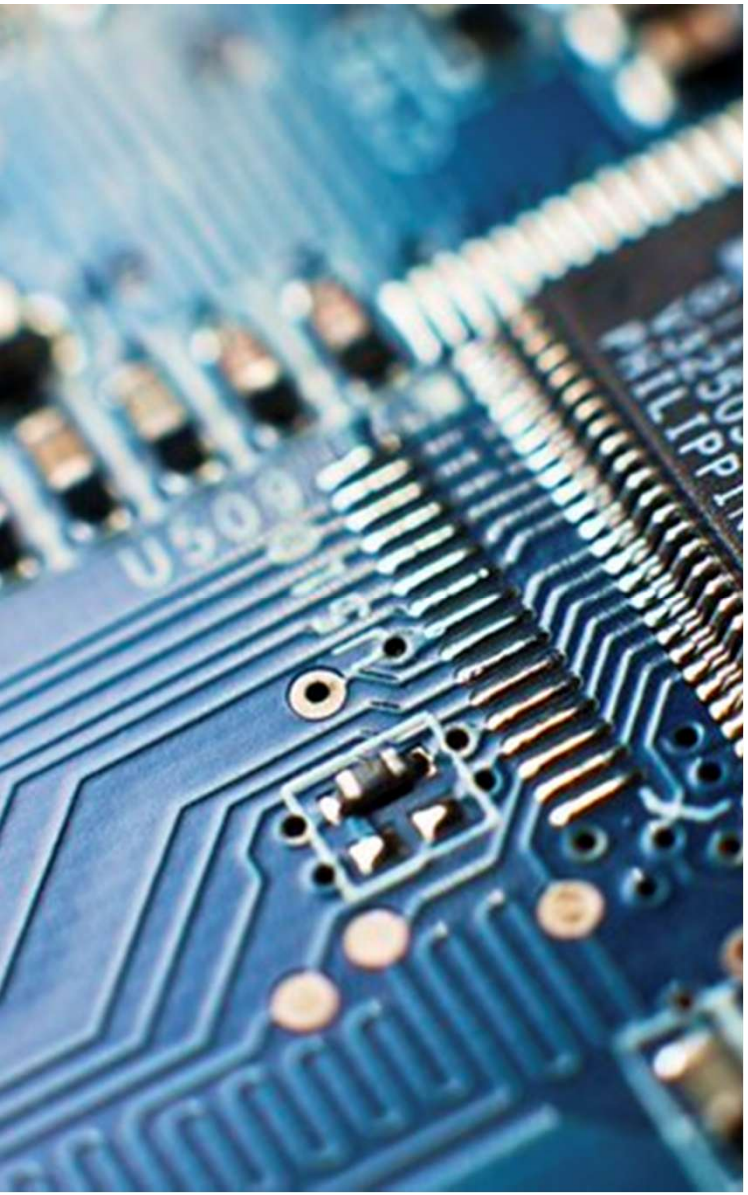
THE COSTLY COMPROMISE

- The Director of Ops of the org gets a social engineering phone call claiming to be the bank
- Caller has deep knowledge of org processes and transactions
- They keep the Director on the phone for more than two hours
- Eventually gain access to financial systems and send $800,000 in wire transfers
- The organization suspected an email compromise had occurred, giving the Threat Actor the information needed to make the social engineering effective
- We were asked to determine if there was evidence of a compromise



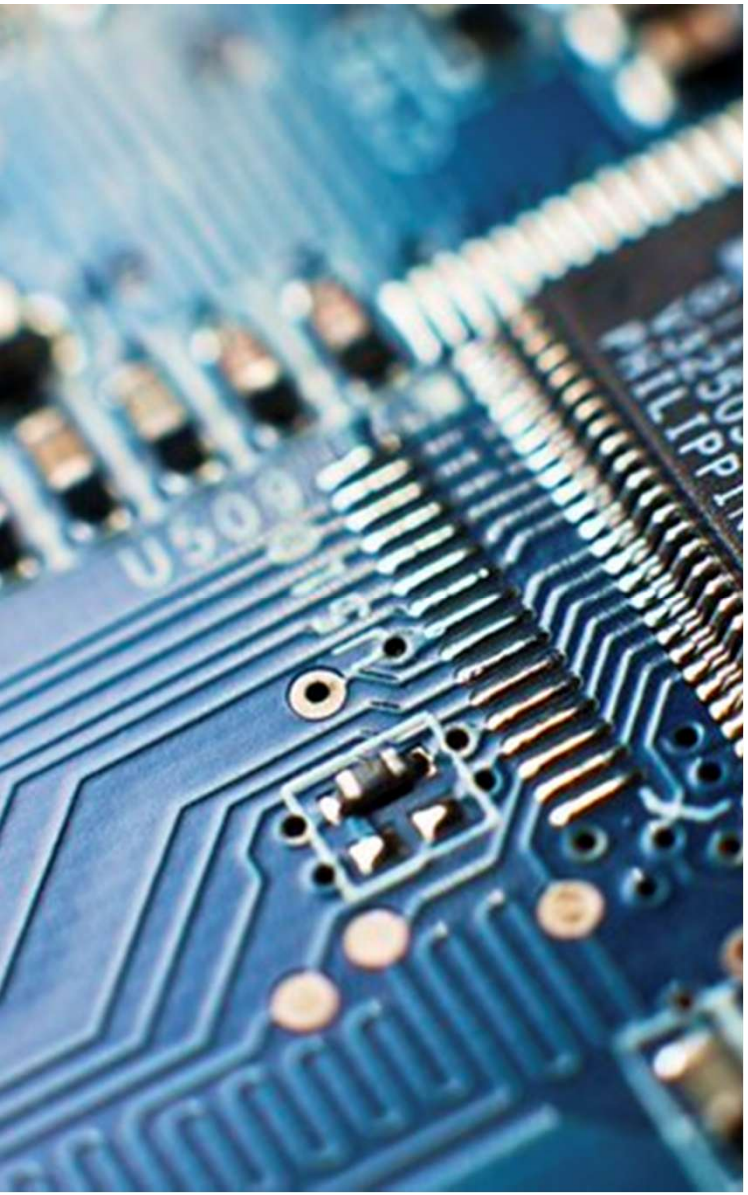
FORENSIC TIDBIT

- The UAL logs IP addresses of many of the activities, allowing for potential geographic placement of the user or actor
- This can allow investigators to determine (in some cases) which account activities are the legitimate user, and which are the Threat Actor.



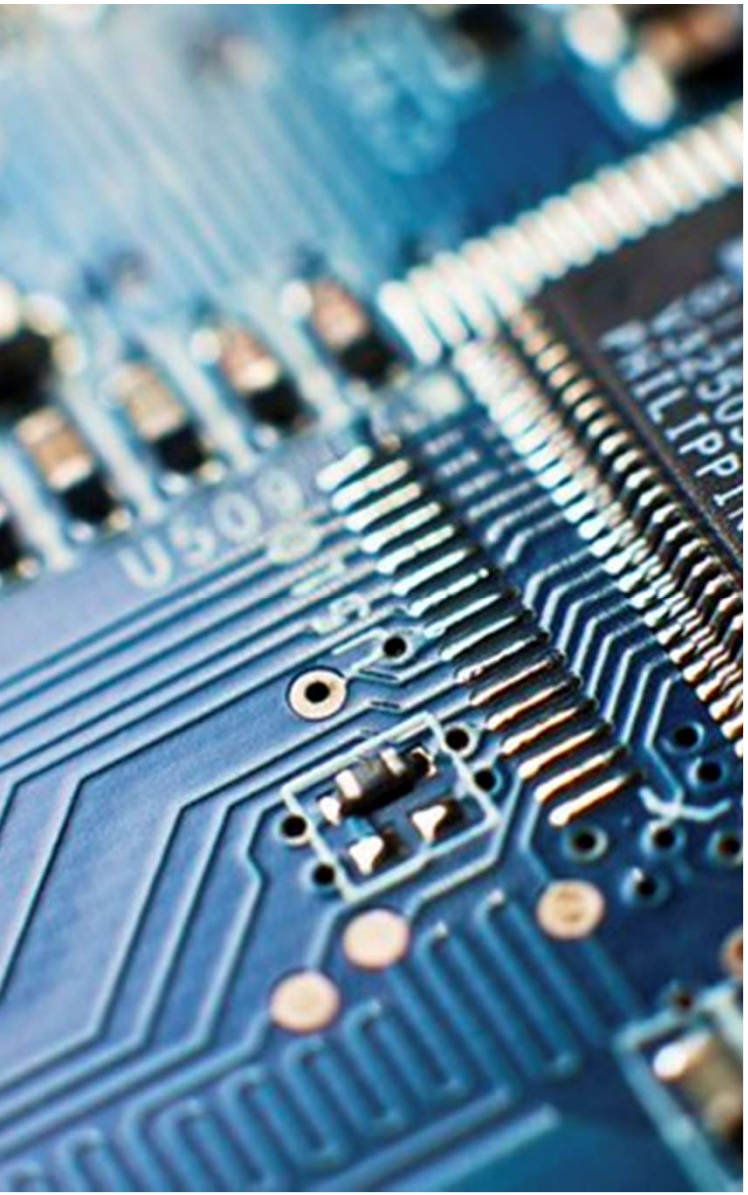
INVESTIGATION QUESTIONS

- Is there evidence of an email compromise?
- Which accounts are affected?
- When did it start?
- How did it happen?
- What did the Threat Actor do while in the system?



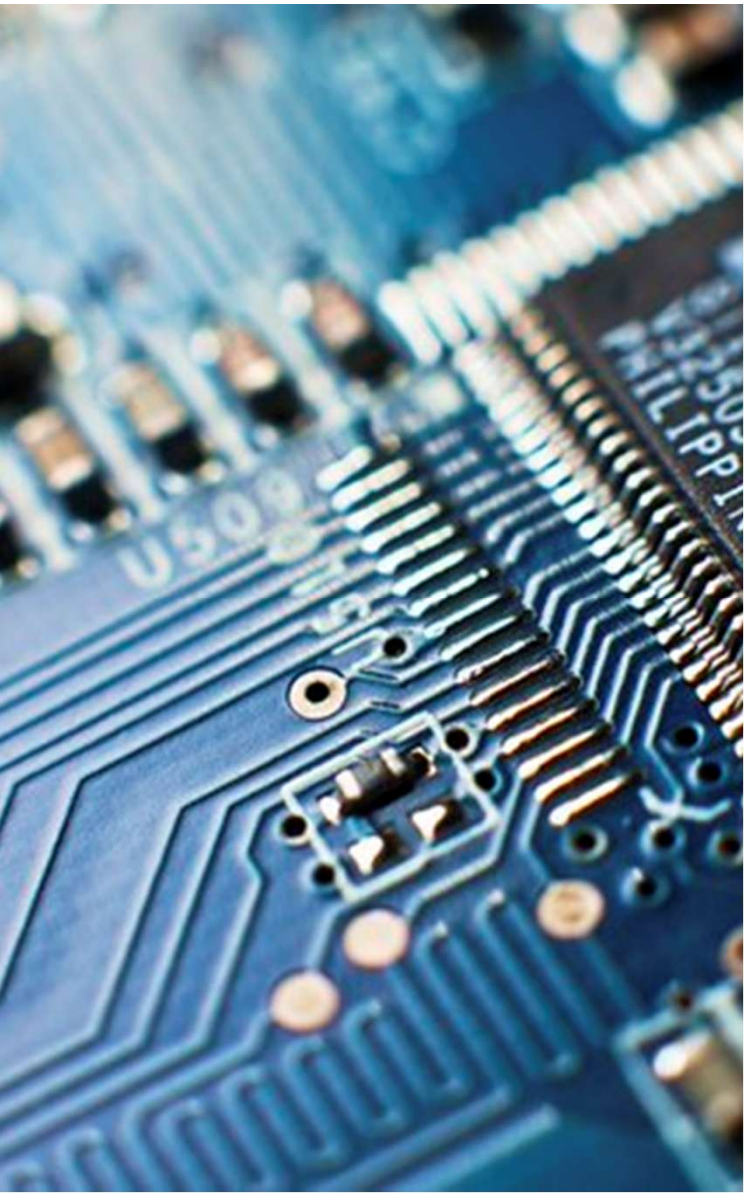
INVESTIGATION RESULTS

- An email account compromise did take place leading up to the attack.
- The original attack occurred outside of the log retention period and we could not discover the initial vector or all TA activity due to the missing logs
- Only one account was affected
- More than 300 individual emails were accessed



AFTERMATH

- Some funds were recovered
- Gaps in the system were sealed
- Training program put into place.

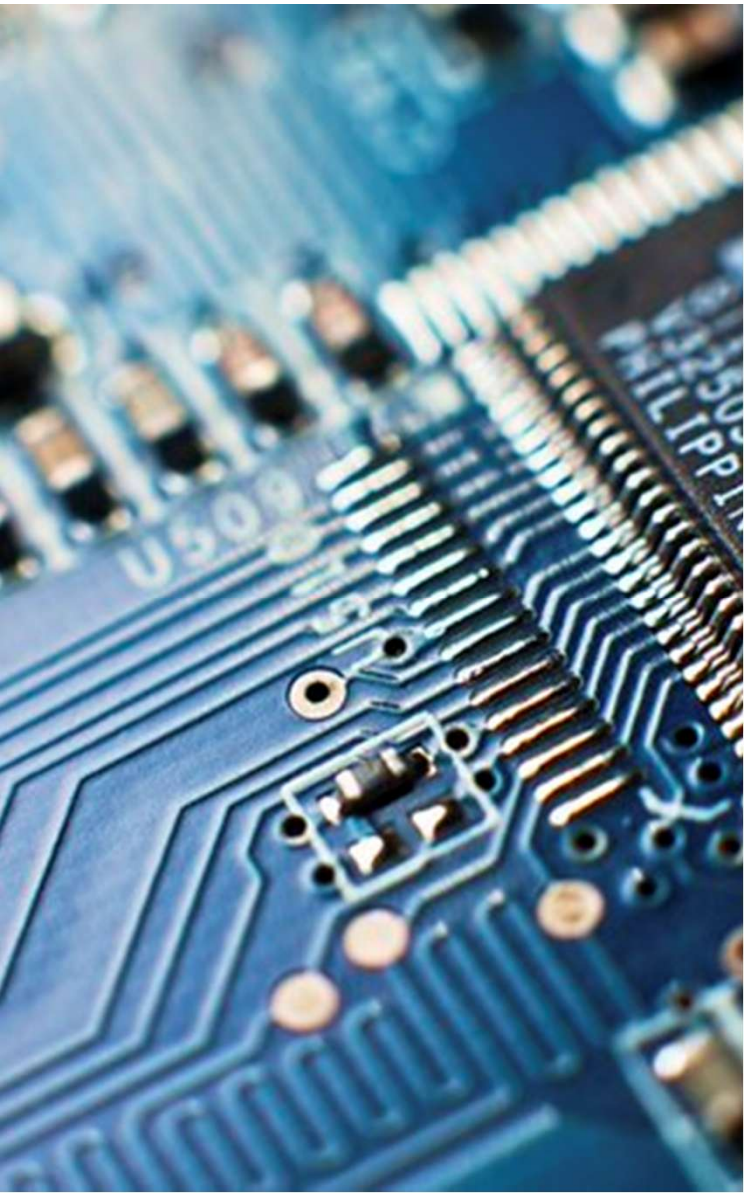


LESSONS LEARNED

- Missing evidence can’t be processed
- Layered defenses are critical
- Detection is as important as prevention
- Don’t ignore internal controls

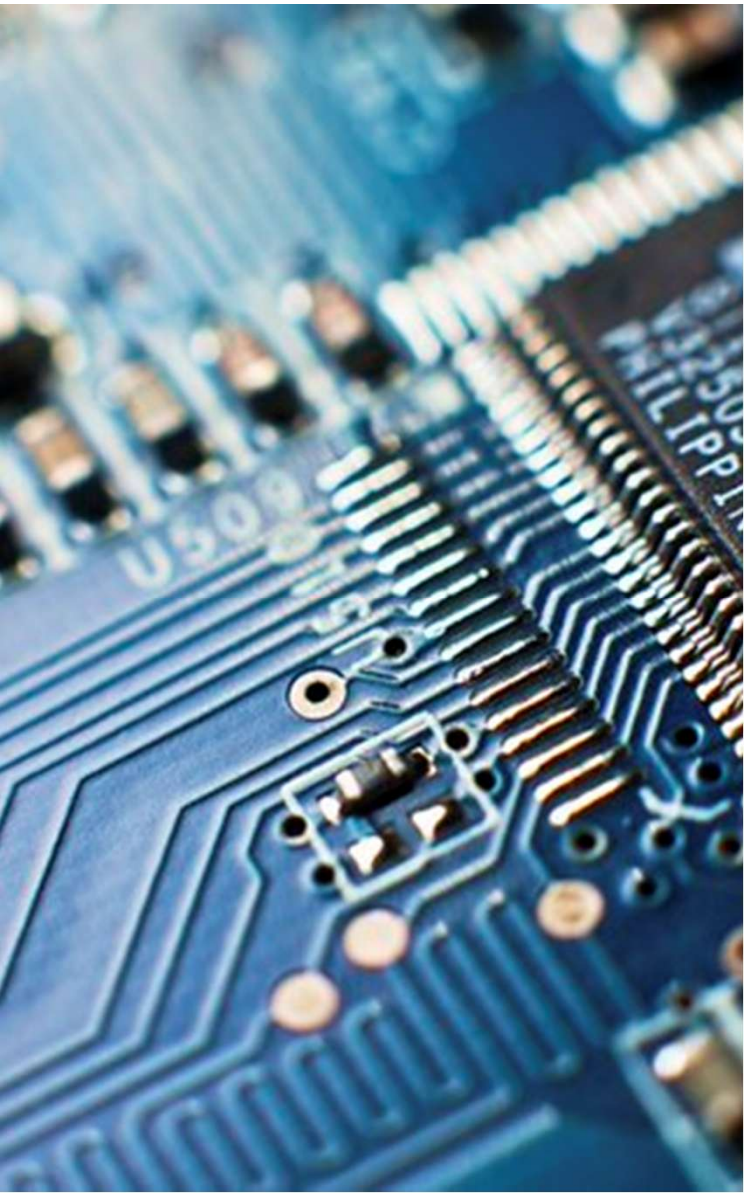
POLLING QUESTION THREE

HAVE YOU REVIEWED YOUR EMAIL SECURITY IN THE LAST YEAR?



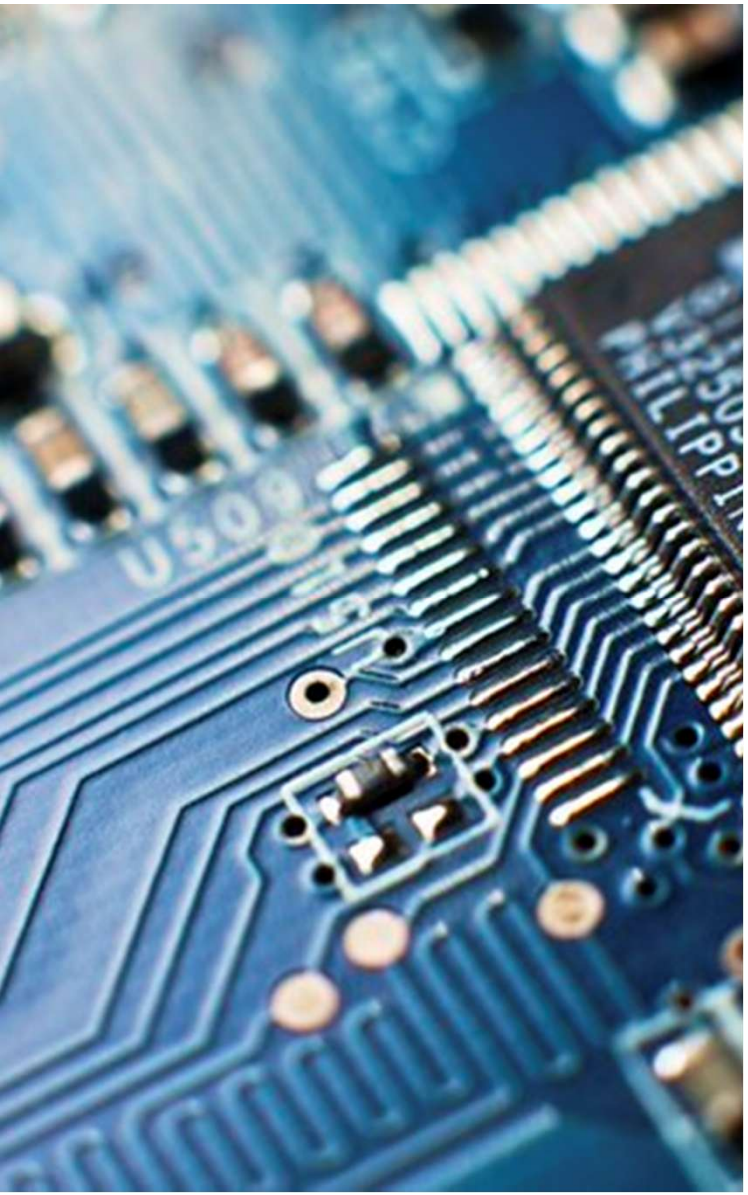
FOUR GOALS OF AN INVESTIGATION

- Preservation
- Containment
- Analysis
- Recovery



DIY OR GET HELP?

- How likely is litigation?
- How serious is it?
- How complicated is it?
- How skilled is our in-house expert?
- How expensive will it be?



BASIC PREVENTION

- Overall cyber review
- User training
- Multi Factor Authentication
- Prevention settings
- Detection settings
- Response preparedness

THANK YOU

Stu Deken

314.678.3737

stewart.deken@rubinbrown.com

www.rubinbrown.com/cyber

WELCOME TO THE 11TH ANNUAL HACKING CONFERENCE

Check-In Code: sweepleg

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter