

Cybercrime Attack Board of County Commissioners Update



STRONG

December 12th, 2017

*"Accelerating Speed to Strategic Value
Utilizing Quarterly Governance"*

Information Technology Services

Agenda

- ❑ What Happened? Cybercrime Incident
- ❑ Cyber Incident Response Plan Execution
 - Phase 1: Preparation
Make & Be Ready to Respond
 - Phase 2: Detection
Identify & Respond
 - Phase 3: Analysis & Validation
Investigative Process for Digital Forensics
 - Phase 4: Containment, Handling & Eradication
Utilizing a Controlled, Methodical, Secure Process
 - Phase 5: Recovery
'New Normal' Standard Operating Practices
- ❑ Post Recovery: Need to Accelerate Securing the Business Platform 3-Year Plan
- ❑ How Could This Happen?

CYBER SECURITY THREATS ARE RISING

SOCIAL ENGINEERING
The clever manipulation of the natural human tendency to trust.



Social Engineering

TYPES OF ATTACKS

PHISHING	SPEAR PHISHING	VISHING
SMISHING 	MINING SOCIAL MEDIA 	LEARN MORE

www.vasco.com/crontosign

Baiting

Tailgating

Pretexting

What Happened? Cybercrime Incident (What we know at this time)

Note: Fortalice Solutions is performing cyber forensics, which at this point is not complete.

- In early December, Mecklenburg County network credentials were compromised by cyber criminal(s) using a social engineering Phishing attack
- The criminal(s) utilized harvested user sign-on credentials to gain un-authorized access to Mecklenburg County systems
- The criminal(s) then planted Ransomware to 'Freeze' select systems and then demanded payment to 'Unfreeze'

IT Security: Cyber Incident Response Plan - Phase 1

Phase 1:
Preparation

■ Cyber Incident Response Plan

- ✓ Draft plan distributed to key stakeholders - *Complete*
- ✓ Cyber Security Table Top Exercise Scheduled for October 2nd @1pm (LUESA) - *Complete*

Mecklenburg has defined alert, event, and incident for response activities as follows

Incident

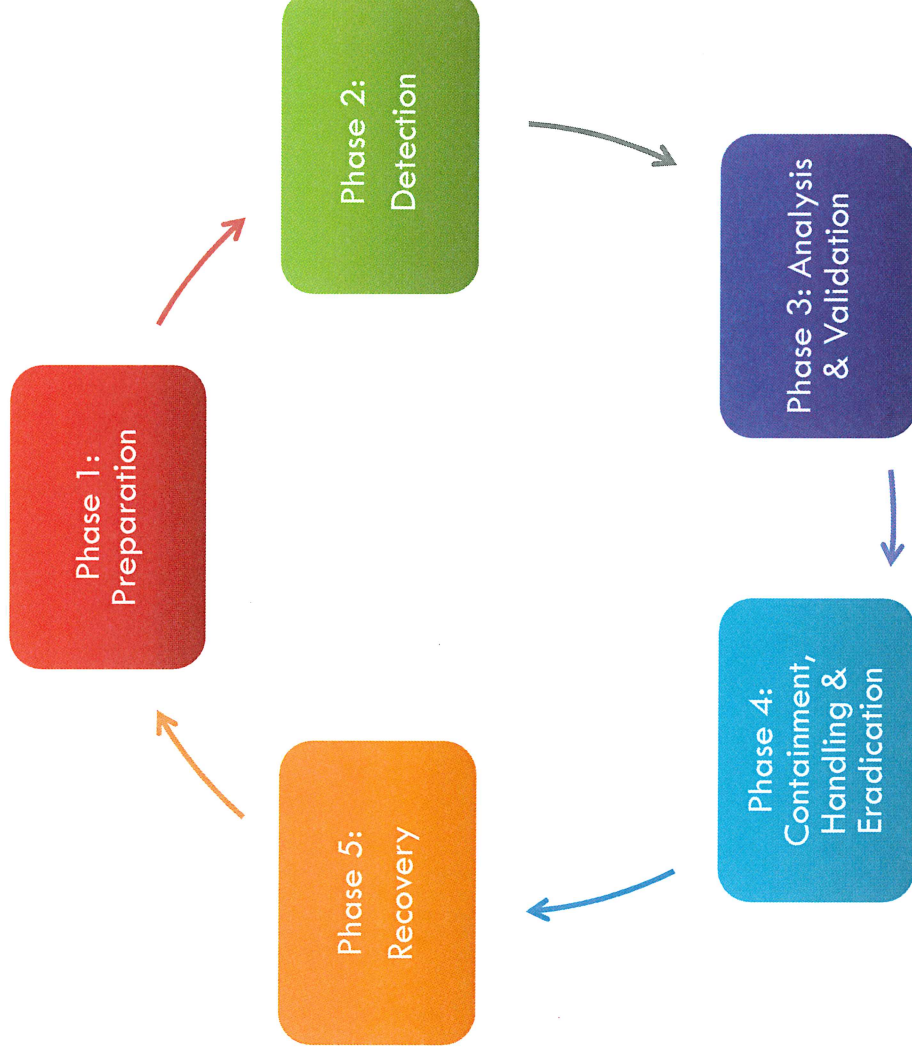
- A major incident is defined as an event which has significant impact or urgency for the business/organization and which demands a response beyond the routine incident management process. The incident poses an imminent threat of violation of information security policies or practices.

Event

- An event is considered verified suspicious activity and will require guidance from the CIO and likely the County Attorney to determine cascading consequences. In the event has significant consequences or additional analysis may be needed, it will be deemed an Incident.

Alert

- An alert will trigger a response from the IT security team to investigate the identified anomaly. An alert can be resolved with assistance from IT and may require escalation to the CIO, but not beyond the CIO.



When did we know this was happening and what did we do to contain the damage?

Dec. 05:

■ Early Morning:

- Server alerts were reviewed which indicated potential malware detection
- The IT Incident Response Team was notified and activated to review the situation
- County Executive Leadership Team and Board notified: Departments implement COOP plans
- Contacted cybersecurity forensic insurance provider (Mullen Coughlin LLC / Kivu Consulting, Inc. in Toronto combines technical and legal expertise to deliver data breach response, investigative, discovery and forensic solutions worldwide)

■ Mid-morning:

- Based on external expert advice and counsel, work to contain spread by shutting of systems and unplug from network
- As requested, we provided ransomware message and a sample files to Kivu
 - Waiting for a response (Note: Current belief is attackers are in a time zone ~5 to 6 hours earlier)
 - We have not confirmed:
 - » Can cybercriminals unencrypt files?
 - » Total cost of un-encryption keys from cybercriminals (One key to unlock all servers? Or multiple keys, perhaps one per server?)
 - » What potential “backdoor” or other risks might have been created?

■ Evening:

- “Clean Room” (very manual activities) strategy to isolate servers (turn off the network interface card) and run various Virus Scan tools as well as look for known signs of ransomware

When did we know this was happening and what did we do to contain the damage?

Dec. 06:

- Backups: Server team stood up a new database environment and we restored database backups for various systems which ran overnight (*evening of 12/5 into morning of 12/6*)
- Gained additional insights from various sources regarding potential risks / benefits of paying ransom
- Based on risk / benefit input from numerous discussions with County Executive Leadership, decision was made and communicated that Mecklenburg County would not pay
- Forensic analysis accelerates with Fortalice Solutions – National cyber experts

Cyber Forensics:

Evidence Collection

- “Certification” of no data leakage
- Characteristics of cyber attack

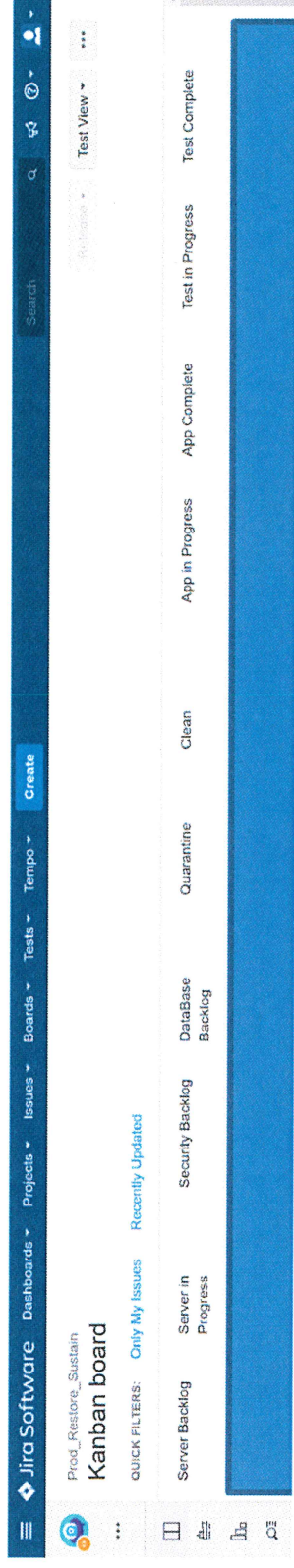


Investigative Process for Digital Forensic Science



Dec. 07:

- Implemented 'Project' Workflow to Ensure Controlled, Secure, Methodical Process:



- Engaged Experts:
 - Fortalice Solutions
 - Microsoft
 - Trend Micro (Antivirus tool)
 - Federal Bureau of Investigation
 - Others

What was the extent of the penetration?

- There are approximately 48 encrypted or infected servers out of 500
- At this time, there does not appear to be any evidence indicating any data leakage

Incident Response Phase 4: Containment, Handling & Eradication

Phase 4:
Containment,
Handling &
Eradication

Dec. 08 – Currently

- ✓ Force reset of all County user account passwords (with extended length)
- ✓ Force reset of all County system accounts
- ✓ Tightened 'In-bound' and 'Outbound' Firewall rules
- ✓ Prioritized Application Servers to initially restore

Restoration Procedures

- Start the server in an isolated mode and disconnected from County network
 - Scan the server using various virus scanning & malware scanning tools
 - Search for certain key indicators in server Registry and file locations
 - Scan backup
 - Indicate whether or not the server is infected
- If not infected
- Connect the server to the network & test
 - Ensure system monitoring tools are installed onto servers
 - Create service design package
 - Collaborate with business to reconcile data gaps and determine business readiness
 - Release application into Production

If infected

- Quarantine
- Rebuild server
- Follow 'not infected' procedures

Incident Response Phase 5: Recovery (16 Systems To Date)

Phase 5:
Recovery

County Prioritized System Restoration (Focus on Public Service)

Restoration Accomplishments (as of 12/11/17, 4PM)

APPLICATIONS RESTORED TO PRODUCTION

- SHF: Arrest Processing (AP) restored on 12/6 - Without AP Tracking
- CJS: PreTrial Case Management System, includes integration with arrest data, does not include court data feed from AOC – restored on 12/6
- CJS: Arrest Processing integration with Pretrial Case Management System – restored on 12/6
- Enterprise: Printing - Ricoh print server restored on 12/7- Departmental secure copy/ print functionality enabled, except Scan to Me functionality.
- CJS: AOC interface to Arrest Processing has been restored (12/8).
- Enterprise: PeopleSoft Payroll in production (12/9) - again, this is payroll only.
- SHF: All Arrest Processing reports restored on (12/11)
- CJS: Jury Manager
- HLT: ECHO
- DSS: Transweb (internal) – the public vendor portal is not yet working
- DSS: ISSI Child Welfare (reporting is not yet available)
- DSS: ISSI Classic (ELF functionality is currently not yet available, requires a small workaround to bypass the Splash application)
- DSS: Just 1 Call
- DSS: Cybervault (was not on priority list but is required for Transweb and ISSI)
- DSS: RAISWeb (reporting not yet available)
- DSS: WER

APPLICATIONS RELEASED TO DEPARTMENTS TO TEST READINESS FOR PRODUCTION

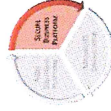
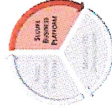
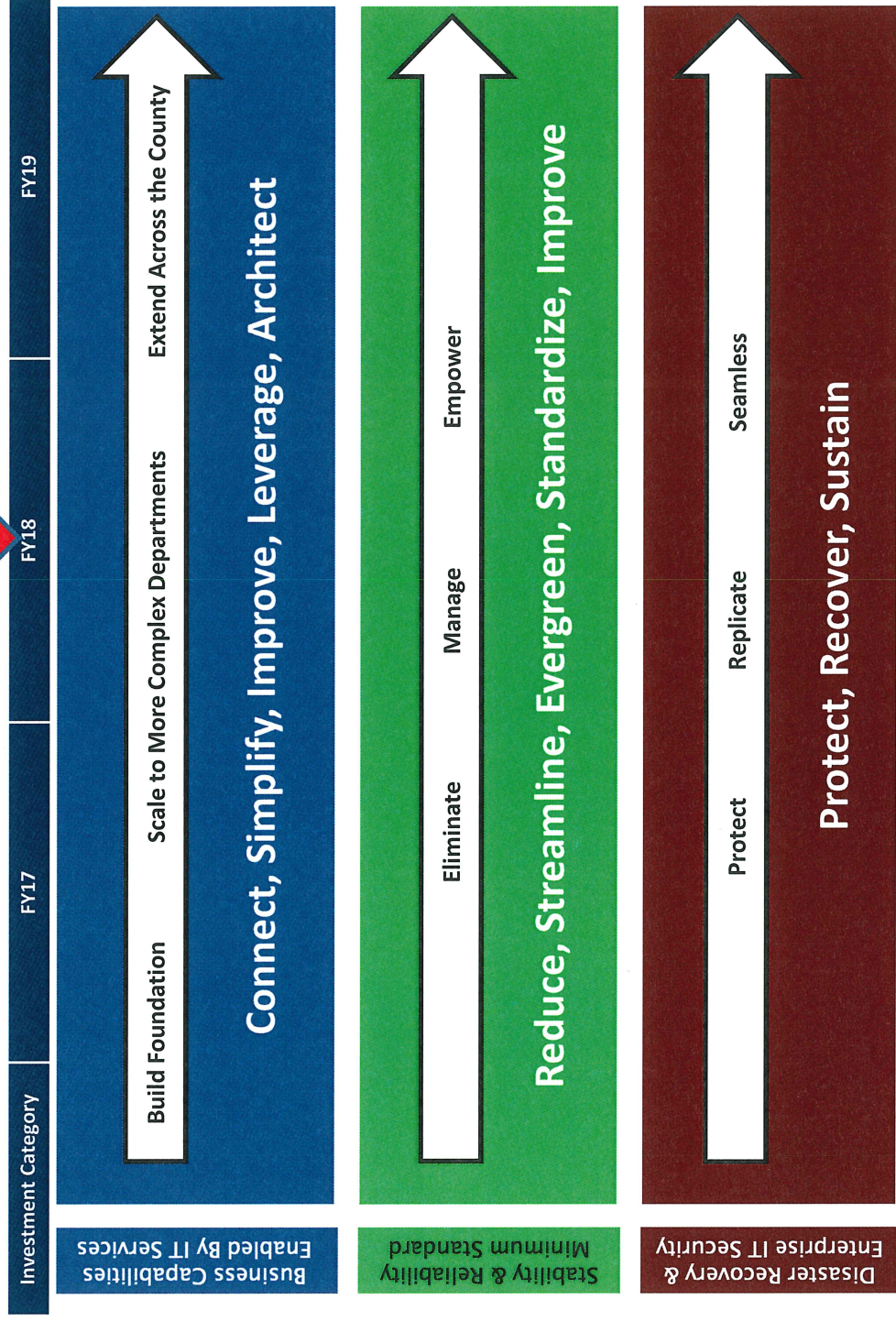
- The following application is with the department testing readiness
- AFM: KeyScan

APPLICATIONS ANTICIPATED TO BE NEXT IN QUEUE FOR DEPARTMENT TESTING

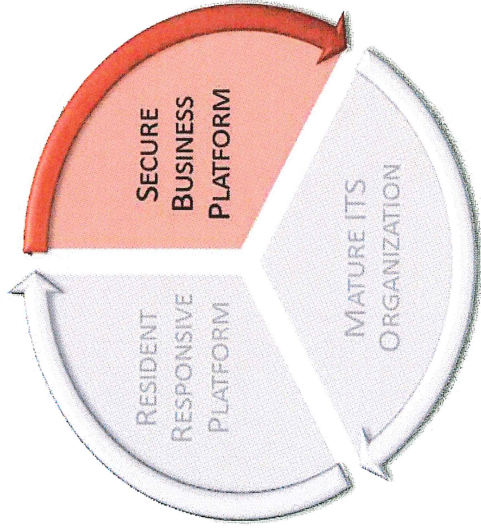
- LUE: POSSE Winchester
- LUE: Navision
- LUE: EPM
- CAO: AssessPro (still confirming)

Post Recovery: Continue & Accelerate 3-Year Strategic Plan

FY19: We are an increasing cybercrime target and we will need to accelerate our strategic plan efforts



Effective Risk Management Requires a Secure Business Platform



Business Capability

Develop application and IT infrastructure recovery plans on a common understanding of essential functions supporting county services

Tools and Process

Secure data and system operations from malicious intrusion and unauthorized use

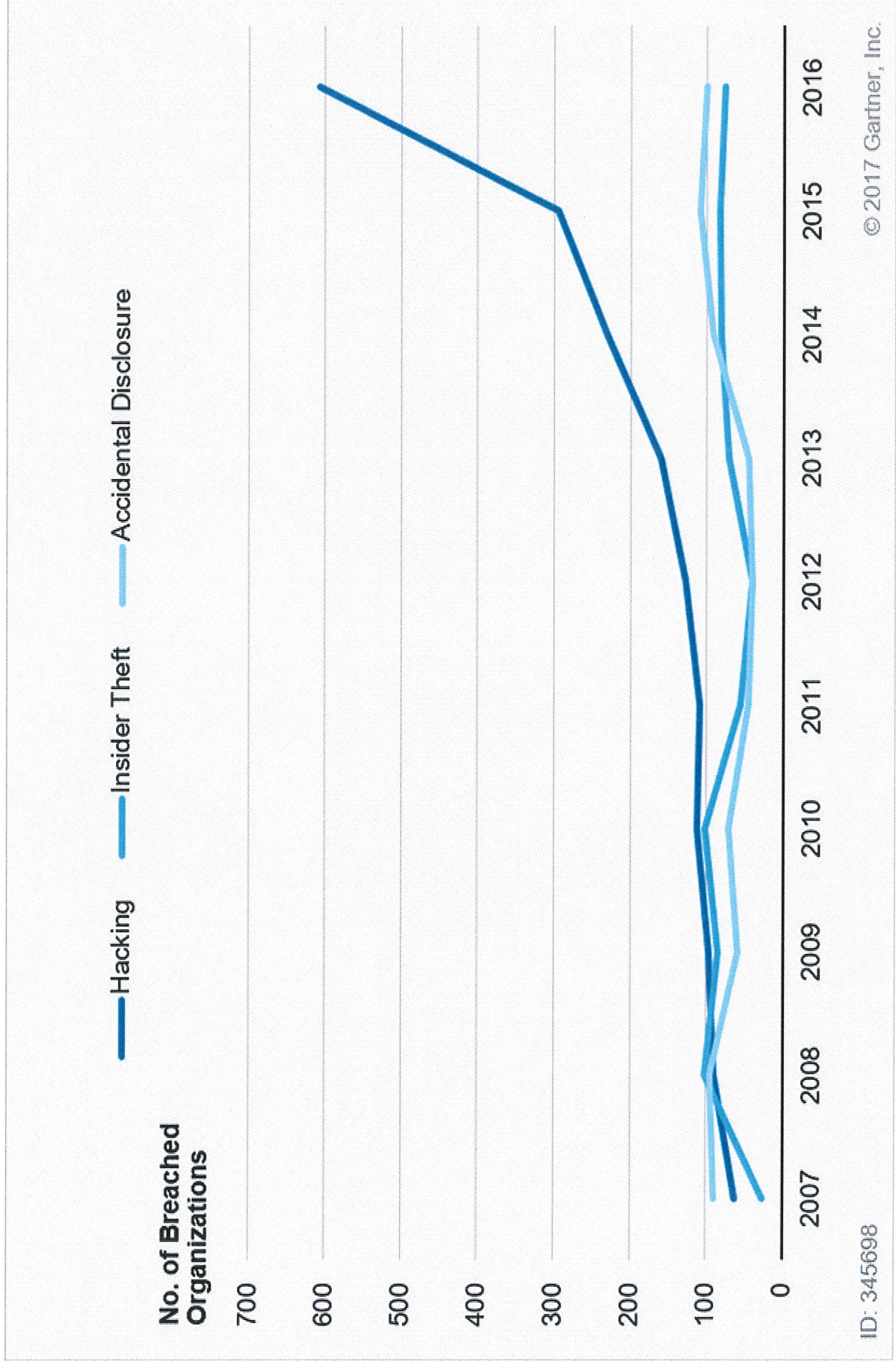
Disaster Recovery

Establish executable disaster recovery capabilities

Infrastructure

‘Harden’ the IT infrastructure against malicious attack, catastrophic mistakes or natural disasters

Number of Organizations in the U.S. That Suffered a Data Breach



RECORDS BREACHED IN FIRST HALF OF 2017

1,901,866,611

NUMBER OF BREACH INCIDENTS

918

Some 1.9 billion data records were lost or stolen during the first half, compared with 721 million during the previous six months, an increase of 164%.

PERCENTAGE OF BREACHES
WHERE NUMBER OF COMPROMISED
RECORDS WAS UNKNOWN

59.3%

PERCENTAGE OF DATA BREACHES
WHERE ENCRYPTION WAS USED

4.6%

Identity theft accounted for three quarters of data breaches, an increase of 49% compared to the previous six months.

DATA RECORDS WERE LOST OR STOLEN WITH THE FOLLOWING FREQUENCY

EVERY
DAY
10,507,550

EVERY
HOUR
437,815

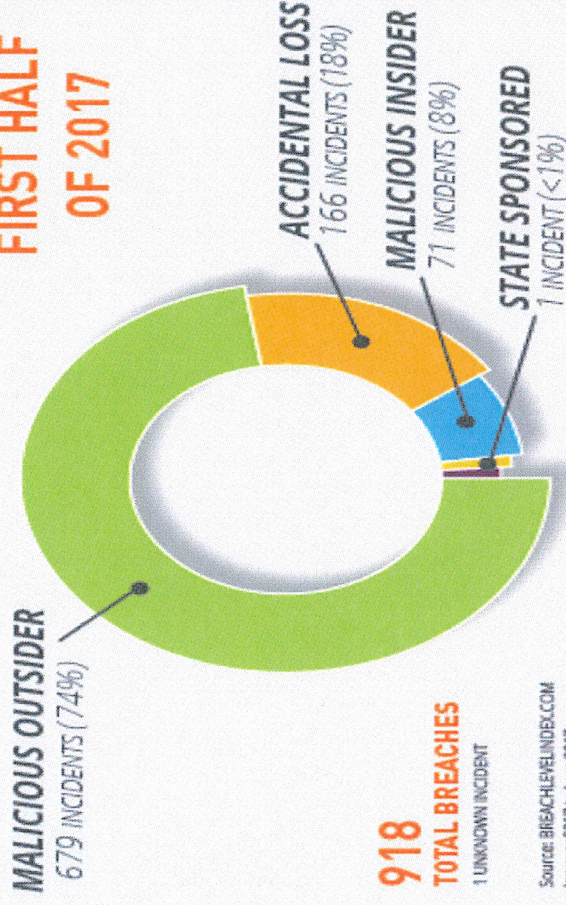
EVERY
MINUTE
7,297

EVERY
SECOND
122

Identity Theft is Once Again On Top

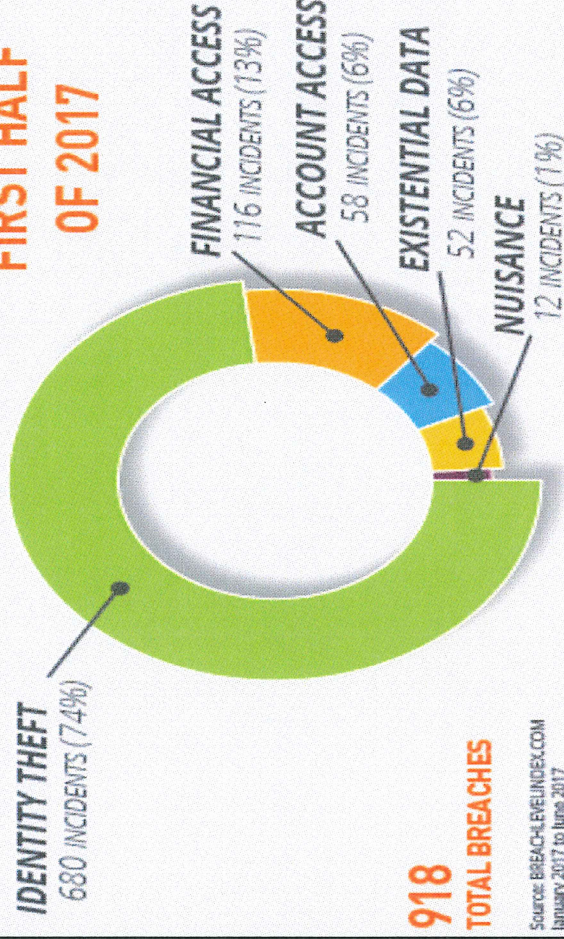
NUMBER OF BREACH INCIDENTS BY SOURCE

FIRST HALF
OF 2017

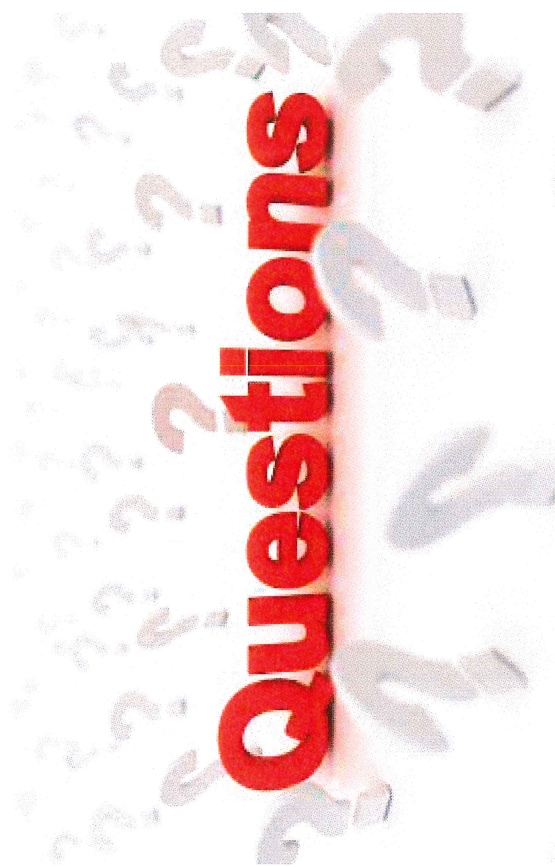
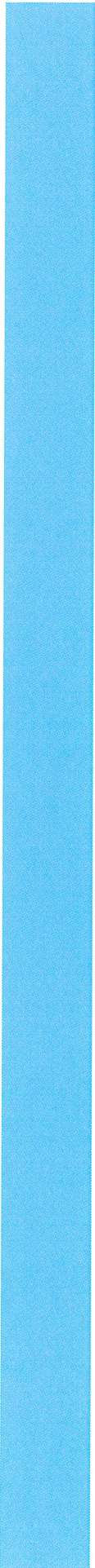


NUMBER OF BREACH INCIDENTS BY TYPE

FIRST HALF
OF 2017



As we've seen in this most recent period, many of the breaches are the result of **accidental loss or inside threats**. A large portion of accidental loss are the result of **poor internal security practices or unsecure databases**.



Questions