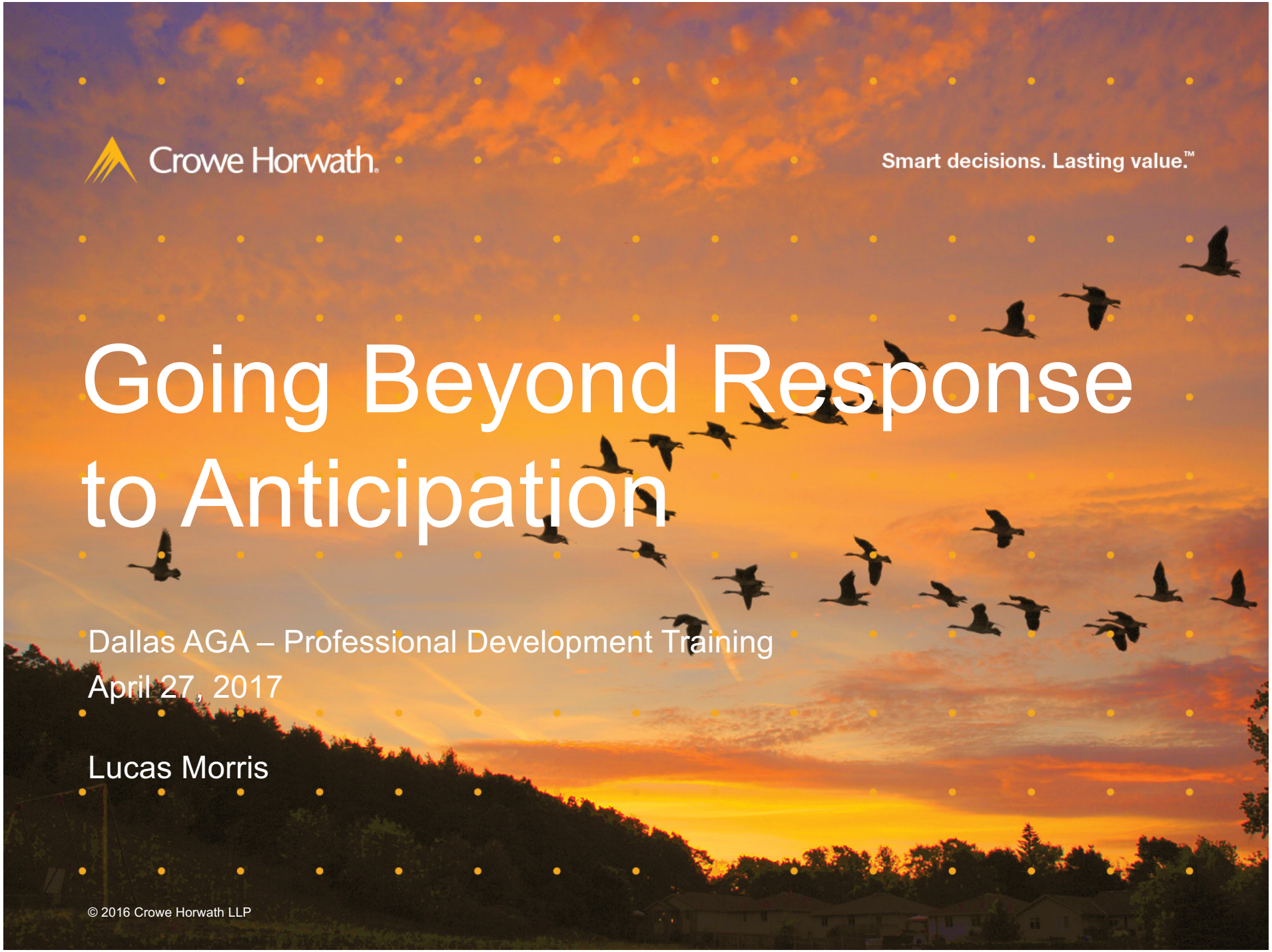
BIOGRAPHY

Lucas Morris

Lucas Morris is a senior manager at Crowe Horwath responsible for leading application security assessments and penetration testing services. He has over ten years of IT experience, starting on the blue team as an administrator and moving to the red team and into consulting. Lucas focuses on helping clients develop more secure environments through penetration testing, technology reviews, and implementation of security solutions. His free time is often spent developing new tools and methodology, helping out with collegiate security competitions, brewing beer, and building things in his woodshop.


Crowe Horwath
Smart decisions. Lasting value.™
Going Beyond Response to Anticipation
Dallas AGA – Professional Development Training
April 27, 2017
Lucas Morris
© 2016 Crowe Horwath LLP

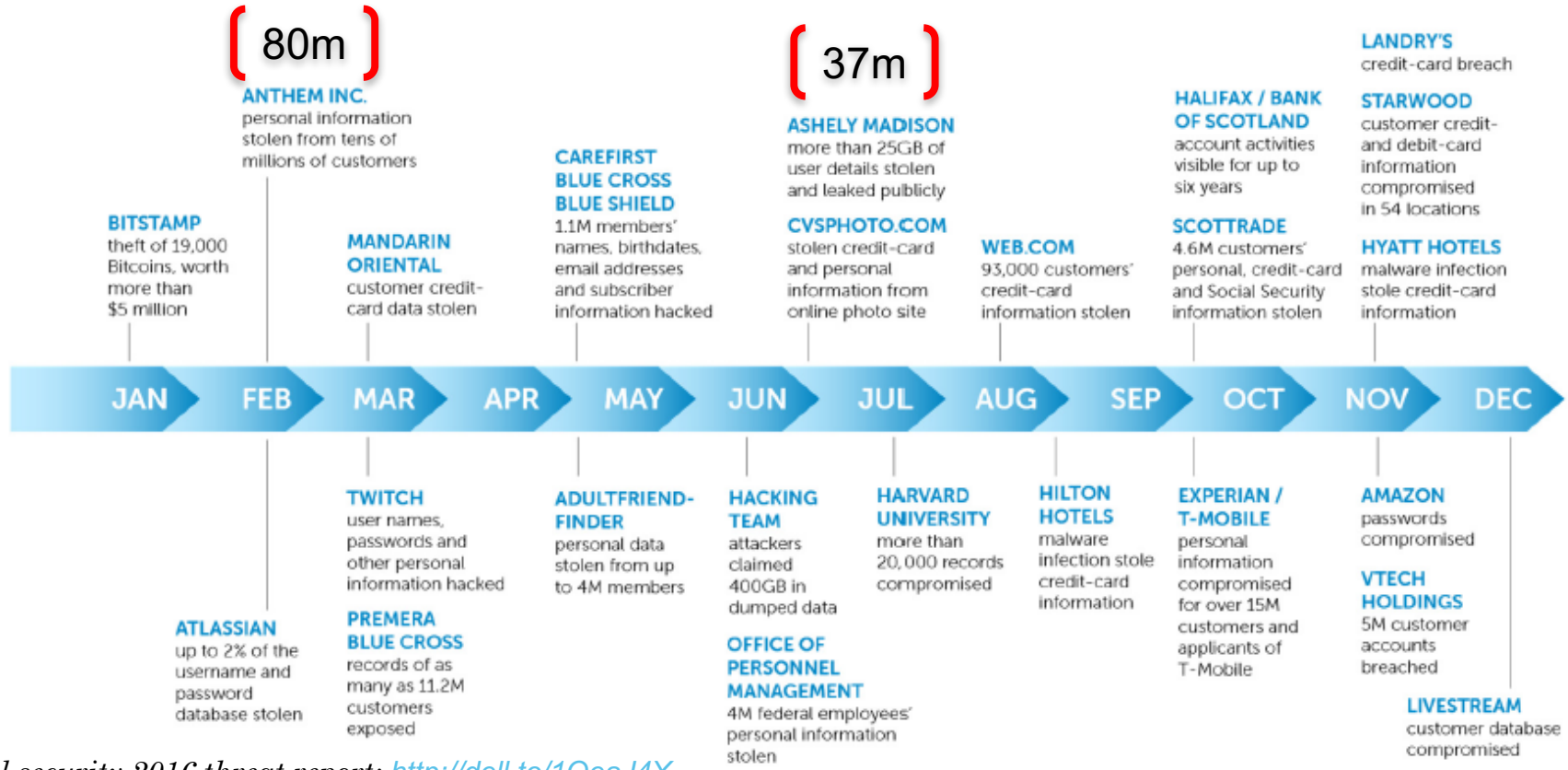
Think Like an Attacker!

<u>Password Policy for Company X:</u>
Length: 8 characters
Complexity Required: Three of the four (A, a, 1, !)
Lockout: 3 Attempts
Lockout Duration: Forever

QUESTION: Given the above password complexity is enabled on the system, what be would ***your first guess*** for user account passwords?

Existing Threats

Breaches By The Numbers



[1] *dell security 2016 threat report:* http://dell.to/1QeaJ4X

Current threat landscape

Attack type trends

- Hacking and malware remain top means of attacks
- Social engineering attacks trend sharply upward
- Slight upward trend of error-based breaches

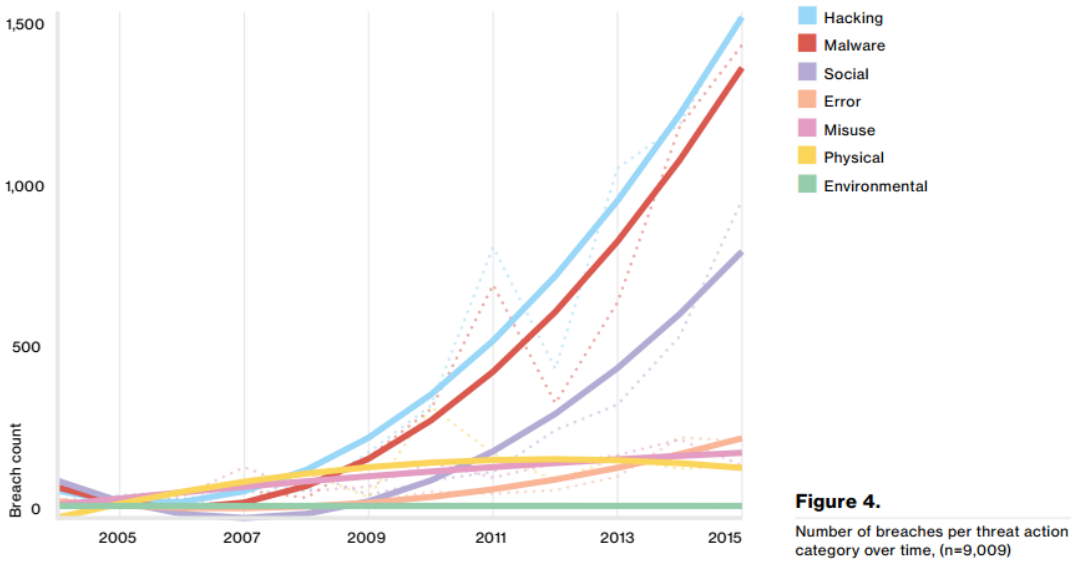


Figure 4.
Number of breaches per threat action category over time, (n=9,009)

Source: Verizon 2016 DBIR – Used with permission

Cybersecurity Threats

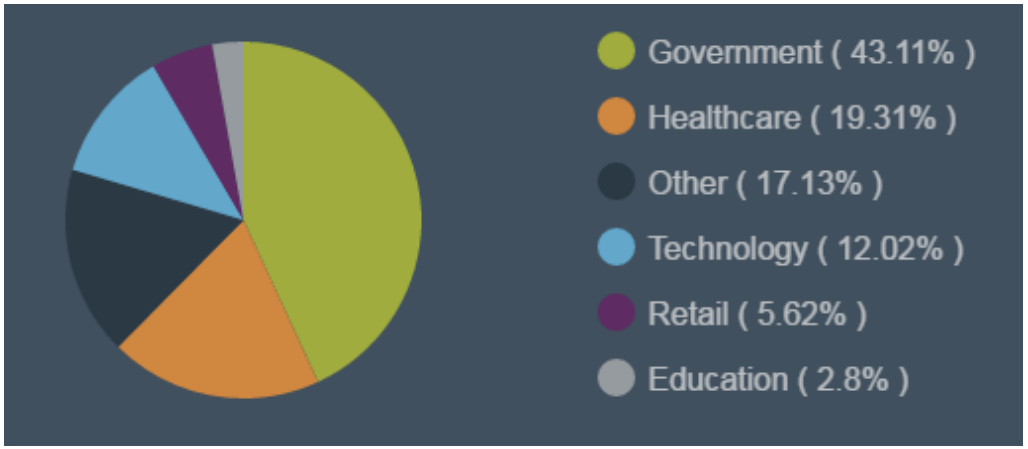
- Who's attacking me?
  - ~80% of all breaches are due to external actors
  - ~20% from insider actors
- Why?
  - ~80% for financial gain
  - ~15% espionage
  - ~5% all else (ideological, grudge, fun)

- Upwards Trending Threats
  - Ransomware
  - Business Email Compromise

Source: Verizon 2016 DIBR

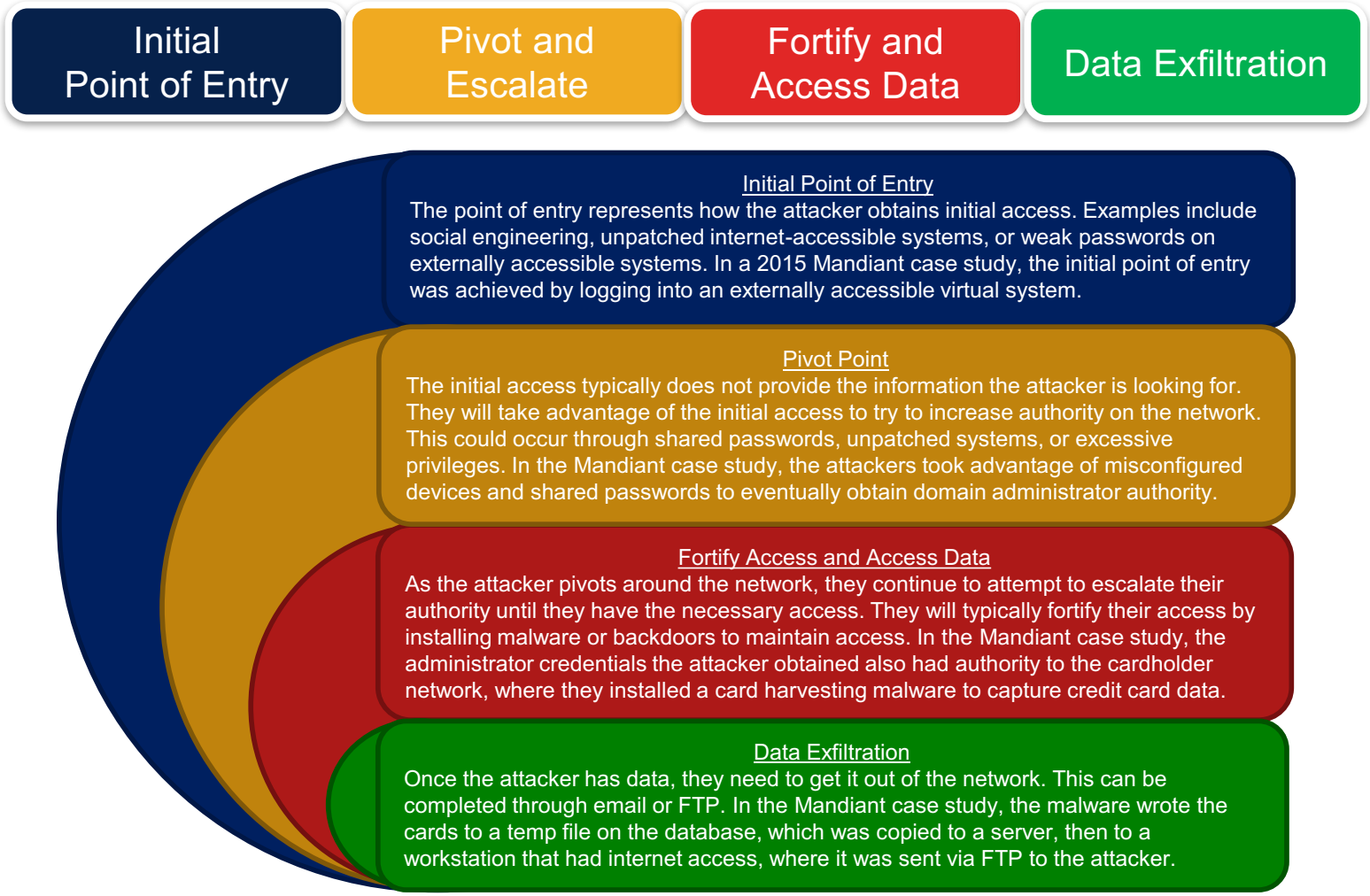
Breaches By The Numbers

- Government
- Healthcare Providers and Insurers
- Higher Education
- Business
  - Software Companies
  - Retail
  - Major League Baseball Team



The Anatomy of a Breach

How do breaches happen?

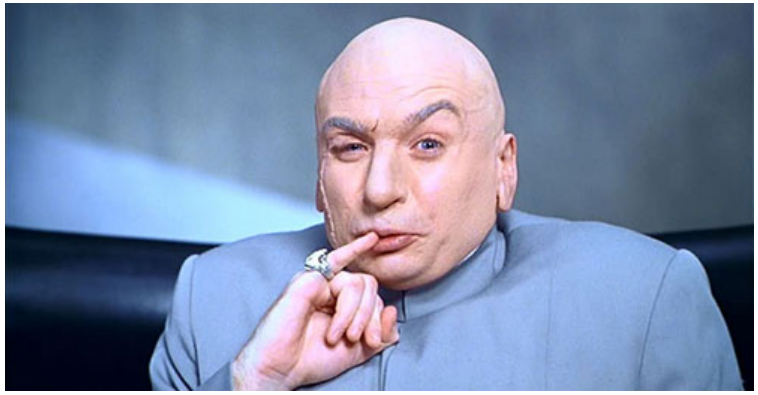


Source: "M-Trends 2015: A View From the Front Lines," Mandiant, 2015, https://www2.fireeye.com/WEB-2015RPTM-Trends.html

Step 1 – Initial Point of Entry

- The first step in any attack is gaining access to *something*:

- The goal is to:
  - Gain a foothold or beachhead to attack from
  - Compromise some level of access, preferably a user account
  - Don't rock the boat



Step 2 – Pivot and Escalate

- Enumerate The Network Setup
  - Identify what is nearby or, if you can make some noise, the network subnets
  - Use network routing protocols (ex: EIGRP / OSPF) protocols
  - Domain Name Service (DNS)

- Identify the Directory and Controllers
  - Enumerate users and groups
  - Enumerate systems and servers

- Identify targets nearby that you can access
  - Reused local administrator passwords
  - Reused authentication keys
  - Users with local administrator access
  - Misconfigured databases

- Limit the attack surface
  - At the network layer via Access Control Lists (ACLs)
  - At the host layer: Disable services not in use (Netbios/LLMNR)
- Ensure network protocol authentication
- Segment critical or important network segments, such as Databases, PHI, PCI, HR, IT into their own networks.
  - Setup access control lists to actually limit the communication, otherwise you haven't mitigated the risk

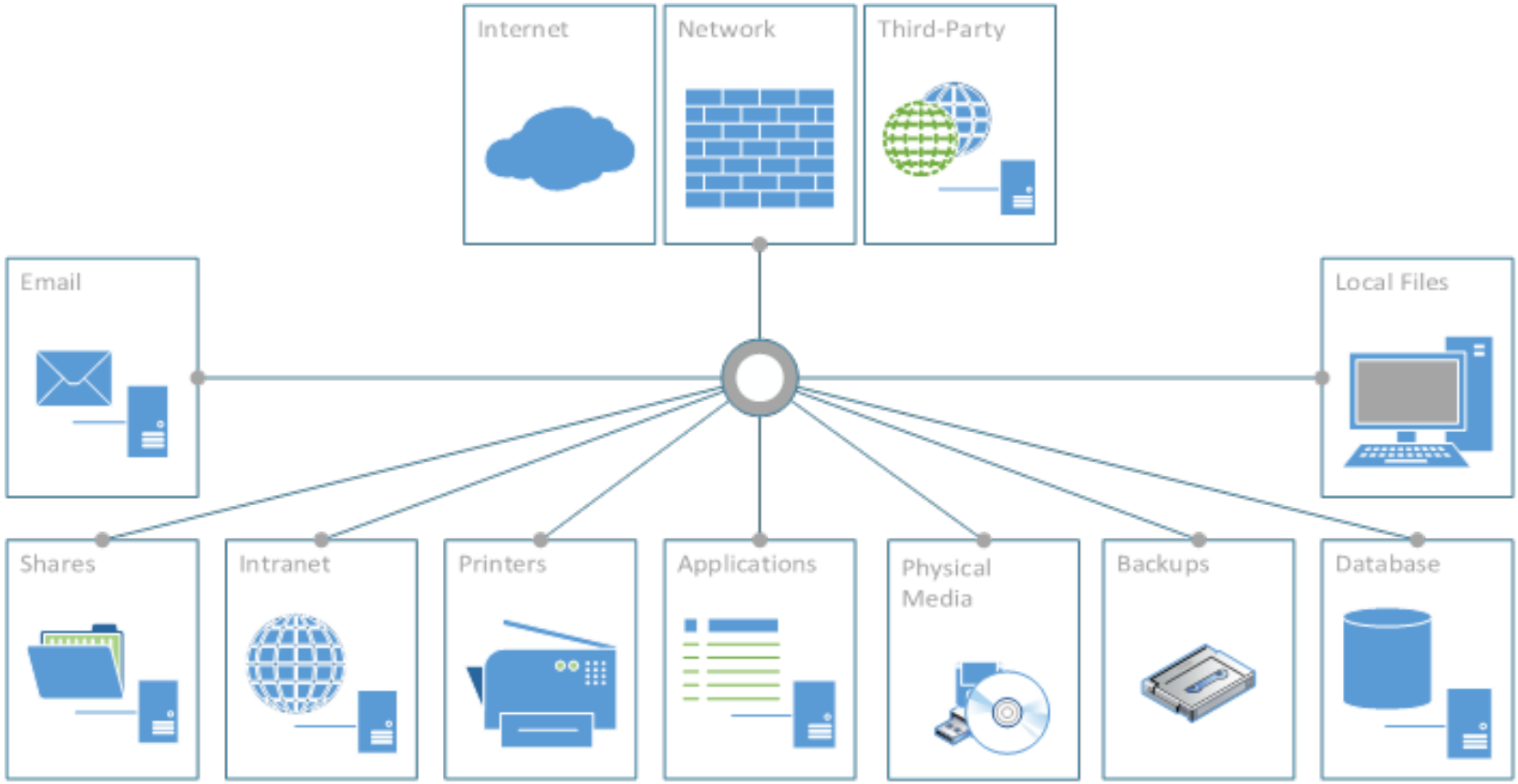
Step 3 – Fortify and Access Data

- As an attacker, it's important to keep activities "low and slow" but this presents a problem

- Access must be made persistent. This can be achieved in many ways:
  - Redundancy by controlling numerous systems
  - Alter system configurations to reconnect regularly, as a scheduled task or on boot
  - Create multiple connections to the same system
  - Introduce additional vulnerabilities

- These all have trade-offs, as they can leave remnants on systems or create network noise

- Time to play the waiting game, looking for data across everything you own



- Weak file shares with permissions allowing full access
- Microsoft SQL Server which allows local OS administrators full database access
- Unencrypted backup tapes or mobile devices (and laptops)
- Lack of outbound network port and web proxy filtering
- SharePoint intranet website without permissions limiting access
- Printers which allow access to recently scanned documents

Step 4 – Data Exfiltration

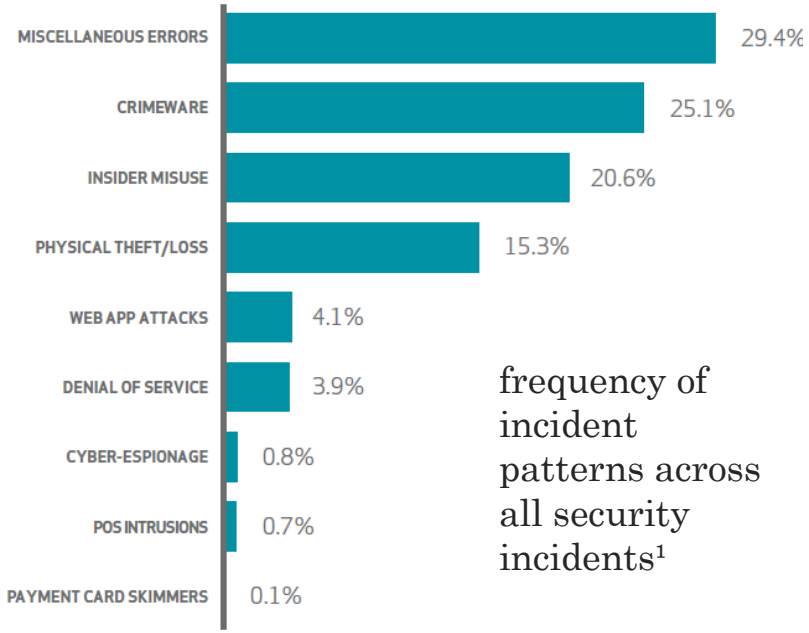
- Data Exfiltration is the process an attacker goes through to get the data out of the network into systems that they control.
- As a few examples, some of the channels attackers use are:
  - Email Services – Including both personal email services (Yahoo, Gmail, Hotmail, etc.) and corporate emails
  - File Transfer Services – Such as FTP, Cloud services (Box, DropBox, OneDrive, etc.), or any file services
  - Network Tunnels – Such as VPN connections to remote solutions
  - Physical Media – USB storage, CDs, etc.
  - Covert channels – Highly technical channels such as tunneling network traffic through DNS or ICMP requests

- Limit outbound data connections!
  - Perform an outbound scan for accessible services
  - What is really required for business?
  - Logging to the rescue – Firewalls allow you to log individual hits.
  - Web proxies allow warning messages for uncategorized sites, or you can block them and require IT approval for access.
  - DNS should be allowed outbound only from actual DNS servers/IT management.

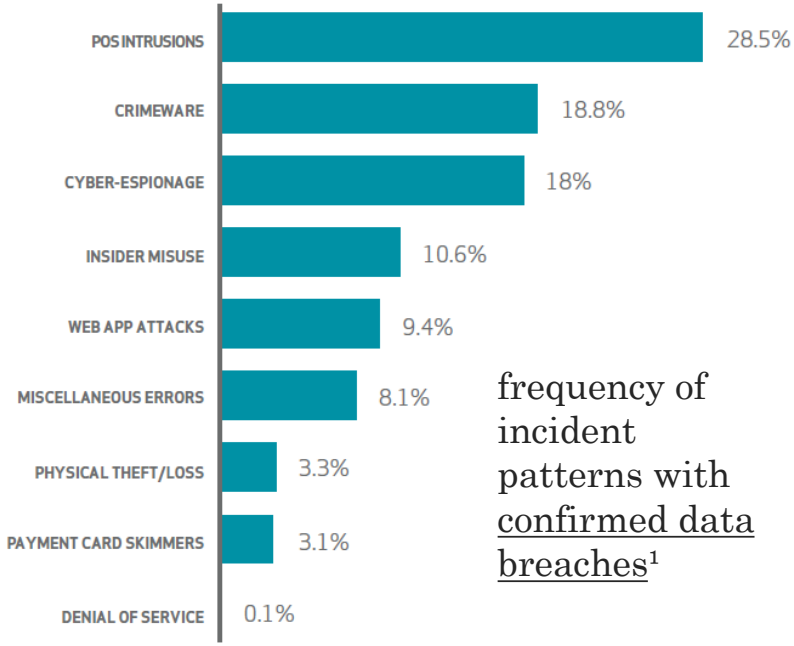
- Data Loss Prevention (DLP)
  - DLP solutions can help to monitor or even stop potentially sensitive information from leaving the organization.
  - DLP is a PROGRAM not a PRODUCT
  - Are you receiving alerts? Does the organization follow up on alerts?
  - Have you tested the program?

Response

Assessing the Relevancy of Threats



frequency of incident patterns across all security incidents[1]

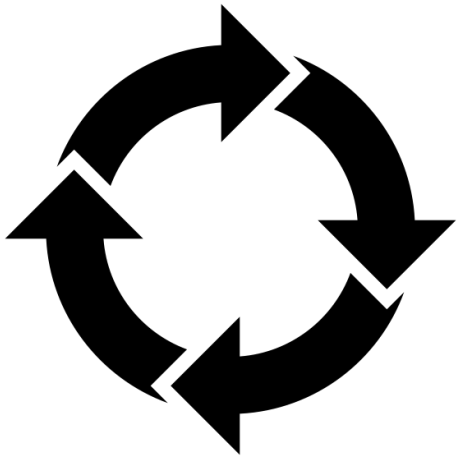


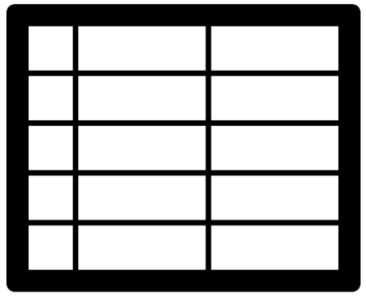
frequency of incident patterns with confirmed data breaches[1]

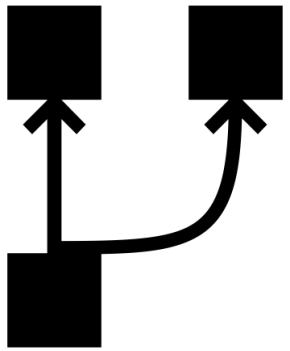
[1] *verizon dbir 2015: http://vz.to/1ILoZPv*

Identification of Sensitive Assets

- Understand the Data Flow of your Organization
- Create an Inventory of Systems and Assets
- Hold Management Accountable
- Test and Audit Regularly







How Does And Organization Deal With These Risks

- What is the organizational strategy to Information Security?
  - How involved is Management in this strategy?
  - What level of risk are we willing to accept?

- We can no longer expect to prevent all breaches from occurring, so where do we focus?
  - **Detective Controls** – Can I identify breaches or attempts to breach my data?
  - **Data Protection** – How difficult is it to get to my sensitive data?
  - **Incident Response** – Similar to Disaster Recovery, have I tested my plan?
  - **Data Loss Prevention** – What methods are available for an attacker to exfiltrate data to the Internet from my systems?

Information Security Frameworks

COBIT 5	ISO 27001/27002	NIST cybersecurity framework	OCTAVE allegro
- more focus on alignment with business goals, governance roles (2nd & 3rd line of defense) - control set (no risk language) - maps to ISO 27001, NIST CSF	- controls have wider coverage than NIST CSF - accepted standard in many countries - supports certification process - Maps to NIST CSF, COBIT	- subset of verbose sp 800-53 NIST framework - control set (no risk language) - detailed guidance for technical controls - Maps to ISO 27001, COBIT - many publications	- risk-based approach - aligns with NIST risk assessment publication sp 800-39 - Provides steps, worksheets, questionnaires; not a control framework

Thank you.

Please connect with us for any questions or additional information:

Lucas Morris
214.777.5257
lucas.morris@crowehorwath.com