CyberSecurity Trends from 2021 for IA
Targeting Emerging Risks
Senior Manager / Security Practice Lead
Rausch Advisory Services

Background in Information Security, IT Audit, Systems Development, & Database Administration

Fortune 500 Experience:

Built the Global “CyberThreat Unit” for a Fortune 100 including Incident Response, Digital Forensics & Investigations, Threat Intelligence, & Penetration Testing

Leveraged Data Analytics to quantitatively measure risk and security effectiveness through Metrics & KPIs

Joshua C. Sorenson
CISM | CISA

+1 (563) 505-5251
JSorenson@RauschAdvisory.Com
Agenda

• How do we know?
• What did we learn in 2021?
• What does this mean to Internal Audit?
How Do We Know?

- Comprehensive Crime Control Act of 1984
- Computer Fraud and Abuse Act of 1986

"a realistic representation of the automatic dialing and access capabilities of the personal computer."

What sources can we use today?

But… do you think any will give you "a realistic representation…"?
Perhaps there is a better way?
What Did We Learn in 2021?

The leading cause of **Incidents** was **Denial of Service**
The leading cause of **Breaches** was **Social Engineering**

**Basic Web Application Attacks**
&
**System Intrusion**
contributed heavily to both **Incidents** & **Breaches**

Average dwell time - **24 Days**
When detected **Internally** - **12 Days**
When detected **Externally** - **73 Days**

**Ransomware** is a **key ingredient**;
constantly **changing** & **evolving**

Rising focus on compromising **Active Directory**
to create **malicious GPOs**

Source: Verizon Data Breach Incident Report 2021
Source: Mandiant M-Trends 2021
What Does This Mean to Internal Audit?

What is your exposure to Denial of Service attacks?

Have you considered Layer-7 (Application) and Layer-3 (Volumetric) attacks? Do you know the difference? Does your Security Team?

Where are your defenses? Are they effective?
What Does This Mean to Internal Audit?

What is your exposure to **Social Engineering**?

What & where are your controls? Are they **mature**? Are they **effective**?

How do you **know**?

- eMail
- Physical
- Voice
- Web
- Other?
What Does This Mean to Internal Audit?

Average dwell time - **24 Days**
When detected **Internally** - **12 Days**
When detected **Externally** - **73 Days**

*Source: M-Trends 2021 Report*

What is *your* organization’s dwell time?
(*How*) *Do* you calculate it?

What can you learn from your **longest dwell time events**?
Questions?

Joshua C. Sorenson
CISM | CISA
+1 (563) 505-5251
JSorenson@RauschAdvisory.Com