



# Cybersecurity Threat Landscape & MERS Countermeasures



**2019**  
**Annual**  
**Retirement**  
**Conference**

*Presented by: Scott Thompson, MBA CISM*  
*MERS IT, Cybersecurity & Facilities Director*



# Get Your Badge Scanned for Credit!

---

This session has been approved for continuing education credits.



You must get your badge scanned to receive credit for attending!

# Today's Topics

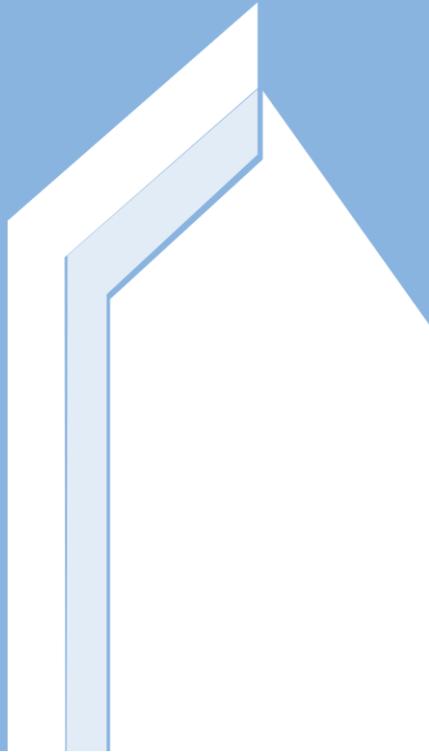
---

## **Cybersecurity Threat Landscape**

- **Common Threat Facts**
- **Real-Life Breach Examples**
- **Social Engineering**
- **Phishing**
- **Threat Severities**

## **MERS Countermeasures**

- **Daily Threats**
- **Cybersecurity Defenses**
- **Cybersecurity Framework**
- **Cybersecurity Collaboration**
- **Future Threat Landscape**



# Cybersecurity Threats

# Common Threat Frequency & Protections

## Unsecure Access

(Login from personal device)

### **FACT:**

**20%** of workers use personal devices for work without permission

### **PROTECTION MEASURE:**

## **Data Encryption**

Encrypt data on devices



[www.core.co.uk](http://www.core.co.uk) - [hello@core.co.uk](mailto:hello@core.co.uk)

# Common Threat Frequency & Protections

## Unsecure Access (Login from personal device)

**FACT:**

**20%** of workers use personal devices for work without permission

**PROTECTION MEASURE:**

**Data Encryption**

Encrypt data on devices

## Stolen / Lost Devices (Laptop/Mobile Misplaced)

**FACT:**

A laptop is stolen every **53 seconds** leaving data vulnerable

**PROTECTION MEASURE:**

**Ability to Remote Wipe Data**

Remotely wipe lost devices



[www.core.co.uk](http://www.core.co.uk) - [hello@core.co.uk](mailto:hello@core.co.uk)

# Common Threat Frequency & Protections

## Unsecure Access (Login from personal device)

**FACT:**

**20%** of workers use personal devices for work without permission

**PROTECTION MEASURE:**

### Data Encryption

Encrypt data on devices

## Stolen / Lost Devices (Laptop/Mobile Misplaced)

**FACT:**

A laptop is stolen every **53 seconds** leaving data vulnerable

**PROTECTION MEASURE:**

### Ability to Remote Wipe Data

Remotely wipe lost devices

## Weak Credentials (Simple, reused passwords)

**FACT:**

**81%** of hacking breaches use compromised credentials

**PROTECTION MEASURE:**

### Multi-Factor Authentication

Verify user before access



[www.core.co.uk](http://www.core.co.uk) - [hello@core.co.uk](mailto:hello@core.co.uk)

# Common Threat Frequency & Protections

## Outdated Antivirus

(Old or dated virus protection)

### **FACT:**

A new malware specimen is released every **4.2 seconds**

### **PROTECTION MEASURE:**

## **Intelligent Defense**

Threat detection /  
prevention



[www.core.co.uk](http://www.core.co.uk) - [hello@core.co.uk](mailto:hello@core.co.uk)

# Common Threat Frequency & Protections

## Outdated Antivirus

(Old or dated virus protection)

### FACT:

A new malware specimen is released every **4.2 seconds**

### PROTECTION MEASURE:

## Intelligent Defense

Threat detection / prevention

## Ransomware / Phishing

(Email ransomware issues)

### FACT:

**91%** of cyberattacks start with a phishing email

### PROTECTION MEASURE:

## Safe Links

Search and strip links of threats



[www.core.co.uk](http://www.core.co.uk) - [hello@core.co.uk](mailto:hello@core.co.uk)

# Common Threat Frequency & Protections

## Outdated Antivirus

(Old or dated virus protection)

### FACT:

A new malware specimen is released every **4.2 seconds**

### PROTECTION MEASURE:

## Intelligent Defense

Threat detection / prevention

## Ransomware / Phishing

(Email ransomware issues)

### FACT:

**91%** of cyberattacks start with a phishing email

### PROTECTION MEASURE:

## Safe Links

Search and strip links of threats

## Leaked Data

(Sharing confidential data)

### FACT:

**58%** of users accidentally share sensitive information

### PROTECTION MEASURE:

## Restrict Access to Users

Only allow specific users



[www.core.co.uk](http://www.core.co.uk) - [hello@core.co.uk](mailto:hello@core.co.uk)

# Common Threat Frequency & Protections

## Outdated Antivirus

(Old or dated virus protection)

### FACT:

A new malware specimen is released every **4.2 seconds**

### PROTECTION MEASURE:

## Intelligent Defense

Threat detection / prevention

## Ransomware / Phishing

(Email ransomware issues)

### FACT:

**91%** of cyberattacks start with a phishing email

### PROTECTION MEASURE:

## Safe Links

Search and strip links of threats

## Leaked Data

(Sharing confidential data)

### FACT:

**58%** of users accidentally share sensitive information

### PROTECTION MEASURE:

## Restrict Access to Users

Only allow specific users

**Greatest risks/threats are from staff members due to accidental, intentional or victim-related vulnerabilities**

# Capital One Breach on Amazon Web Services Cloud

- **Stolen Information**

- 106 million people affected
- 100 million credit applications from 2005 – 2019
  - 140K Social Security numbers
  - 80K bank account numbers

- **“Suspected” Hacker**

- Former Amazon employee
- Openly discussed potential hack plans online with other hackers prior to attack

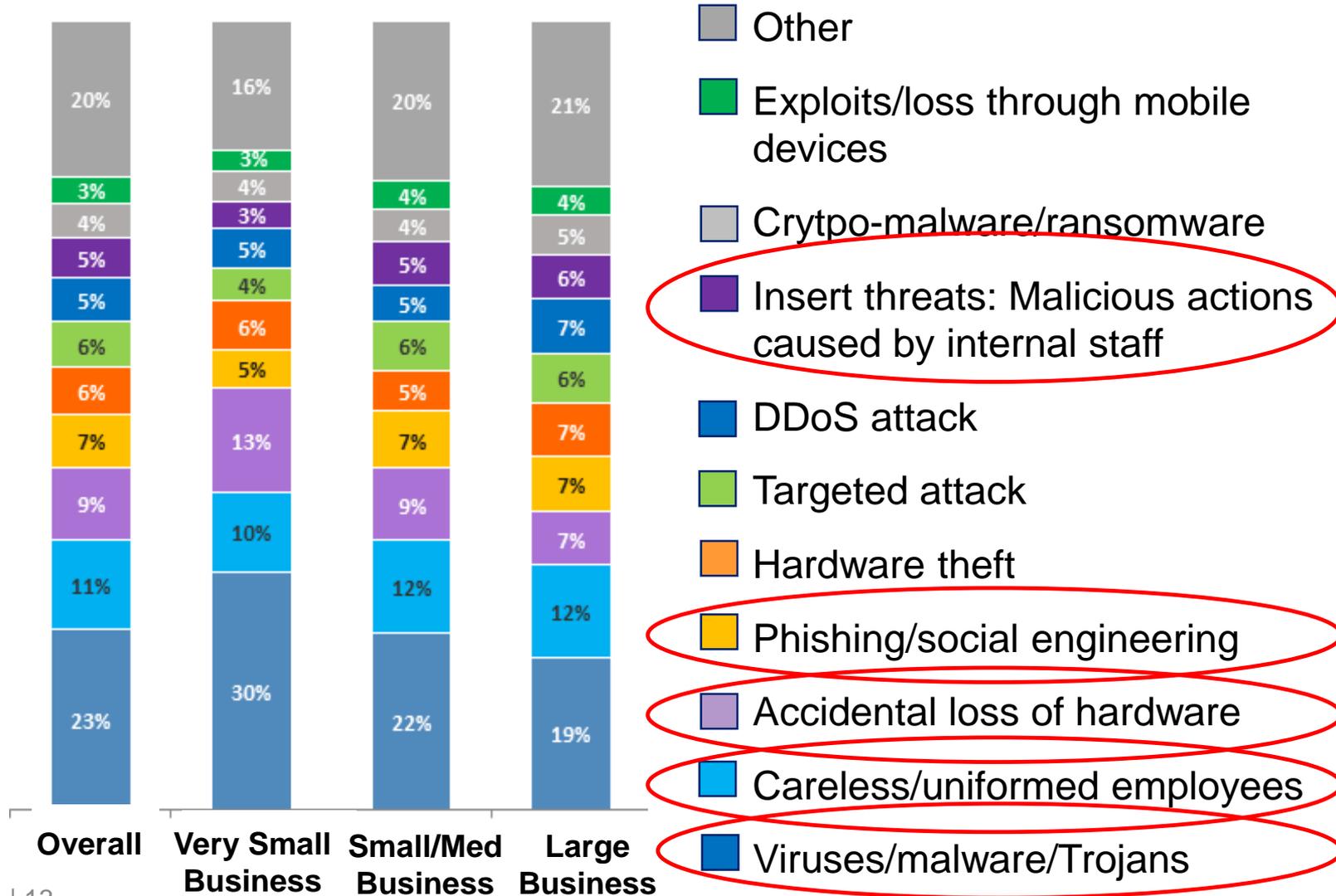
- **“Tip of the Iceberg”**

- Vodafone, Ford, MSU, Ohio DOT and other organizations also hacked



# Organization Size Does NOT Matter...

## Most serious attack vectors



# No Victim Too Small

NATIONAL

## 22 Texas Towns Hit With Ransomware Attack In 'New Front' Of Cyberassault

August 20, 2019 - 10:16 AM ET  
Heard on Morning Edition

 BOBBY ALLYN



Texas state Capitol building in Austin. This week, state officials confirmed that 22 municipalities have been infiltrated and ransom demanded.

EW/Clark/TQ-Roll Call/Getty Images

Source: [www.npr.org](http://www.npr.org)

## Texas Towns Attack

- 1 threat actor/group
- Simultaneous attacks (new)
- Hacked IT support vendor

**State and local governments** becoming more targeted with ransomware attacks

- 169 successful attacks since 2013 (already 60 in 2019)
- Most from overseas sources
- About 17% pay the ransoms

# To Pay or Not to Pay?

## *Ransomware Attacks Are Testing Resolve of Cities Across America*



A handwritten sign posted near City Hall in Baltimore after some of the government's computer systems were hacked in May. The city, which did not pay a ransom of about \$76,000, has spent more than \$5.3 million to recover from the attack. Stephanie Keith/Reuters

Source: [www.nytimes.com](http://www.nytimes.com)

### Who paid ransom?

- Lake City (FL) paid \$460K
  - Avoided recovery costs with cyber insurance

### Who refused to pay ransom?

- Baltimore did not pay \$76K
  - Recovery cost over **\$5.3M** at the time of this article
- Atlanta refused to pay a \$51K
  - Hackers posted attack online
  - Cost of recovery ~**\$17M** at the time of this article

**Ransomware attacks doubled over the past year...cyber insurance and/or ransom payments may be emboldening the hackers.**

# Social Engineering

Use deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes



# Security Awareness Training

Watch the first episode 



# Phishing

Send broad emails that look like they are from reputable sources in attempt to get individuals to reveal sensitive personal information

- Common Types:

- Spear Phishing – Target a group or individual
- Whaling – Target an executive group or individual
- SSMShing – Use text message to manipulate
- Vishing – Use voice to manipulate



# Vishing For Data



**WATCH THIS HACKER  
BREAK INTO  
MY CELL PHONE ACCOUNT  
IN 2 MINUTES**

Pause (k)

0:00 / 2:29



# Phishing Scam Example

From: Municipal Employees' Retirement System <notification@mersofmich.com>  
Reply-to: Municipal Employees' Retirement System <notification@mersofmich.com>  
Subject: Test of the Municipal Employees' Retirement System Emergency Notification System  
MemberPortal.pdf

Template ID: 33869-991061

[Send me a test email](#)

[Toggle Red Flags](#)

This is a message from Municipal Employees' Retirement System Security.

[Please click here to acknowledge receipt of this message](#)

This is a test of the Municipal Employees' Retirement System Notification System. If this were an actual event, this message would contain information about the event as well as appropriate guidance. This is only a test.

**IMPORTANT: If you did not receive this test notification on your mobile device, please [CLICK HERE](#) to add your mobile SMS/Voice to your profile.**

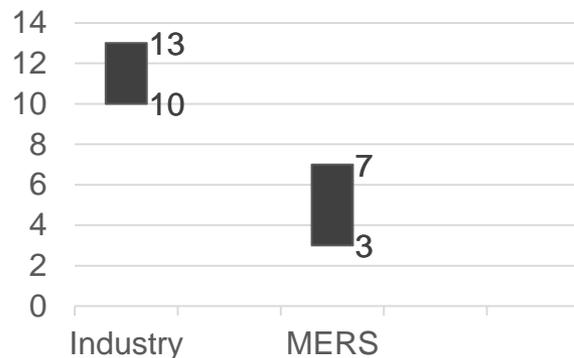
To download the Mobile Application which has enhanced capabilities, view the attachment for more details and instructions for download.

Any questions can be directed to Municipal Employees' Retirement System Security.

If you have received this message in error, please send an email to the System Administrator at [sysadmin@mersofmich.com](mailto:sysadmin@mersofmich.com)

Close

Click Rate (Percentage)

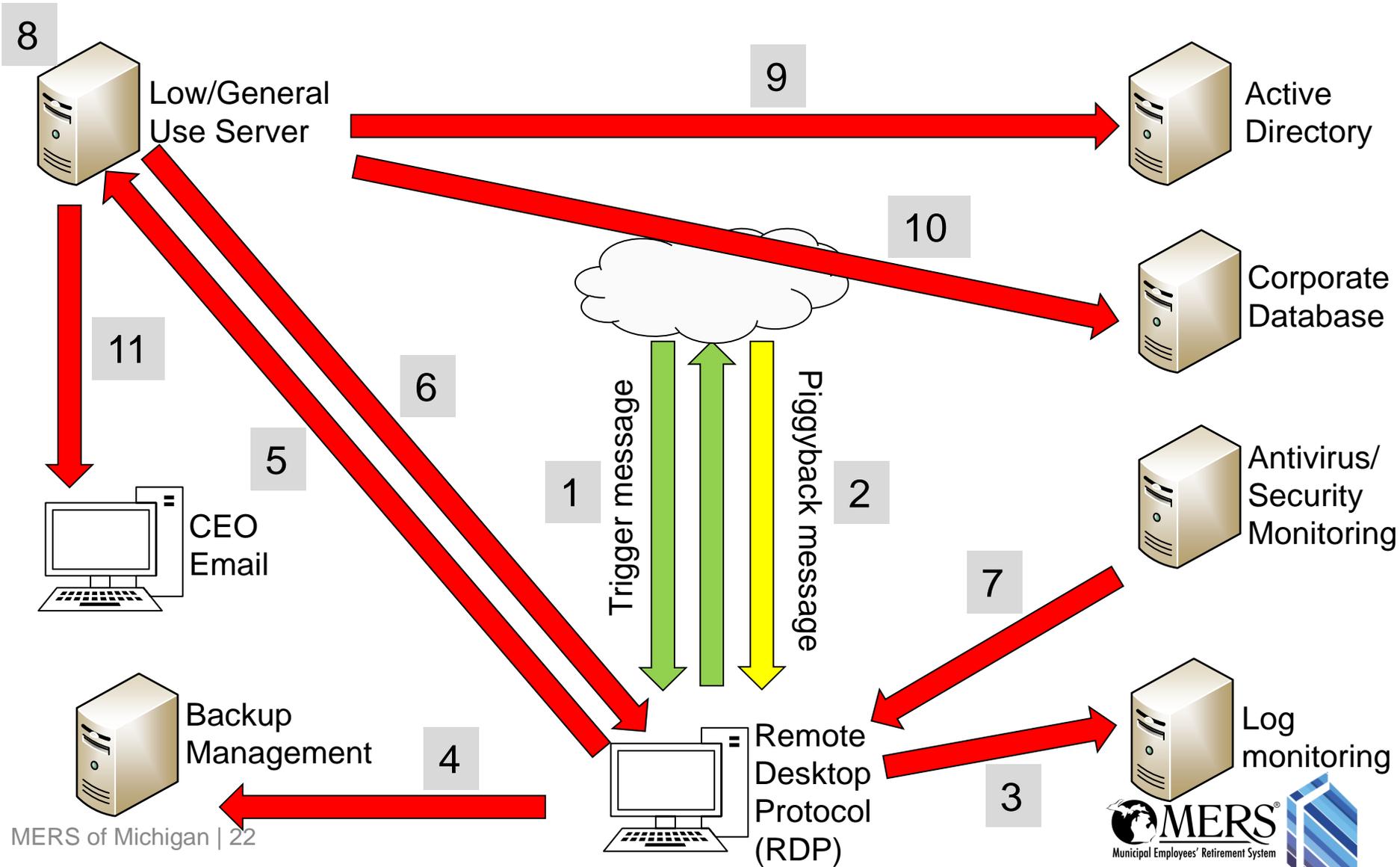


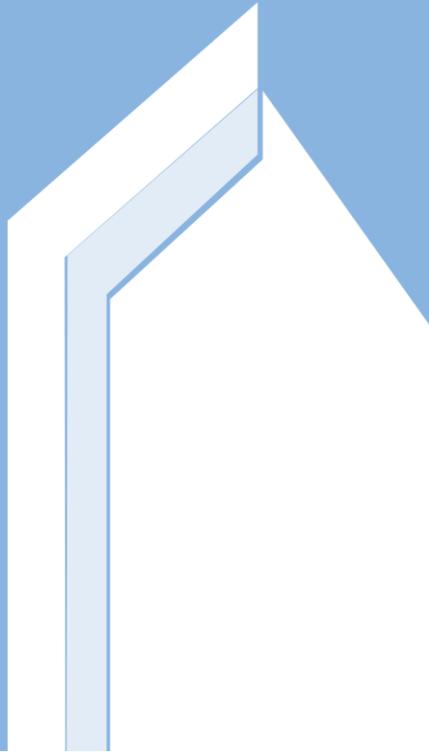
# Security Threat Meter



**Advanced Persistent Threats (APTs)  
typically go undetected for 9 months**

# Anatomy of an APT Attack





# MERS Cybersecurity



# Real-Life MERS Cyber Security Incidents

## Incident vs Breach

- Spoofed emails
- Google.com false alarm
- Training company purchase card incident
- Whaling Emails
- FBI Fraud Alert false alarm

**07 March 2019**  
PIN Number  
**20190307-001**

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:  
[www.fbi.gov/contact-us/field](http://www.fbi.gov/contact-us/field)

E-mail:  
[cywatch@fbi.gov](mailto:cywatch@fbi.gov)

Phone:  
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is

**Private Industry Notification**  
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

The FBI assesses cyber criminals will continue to target participant accounts as well as the systems managed by plan administrators with the intent to steal funds, and will remain an ongoing threat to private industry.

**Recommendations**

The FBI recommends taking precautionary measures to mitigate the threat and protect against exploitation. Employers and plan administrators responsible for managing participant accounts should:

- Alert their workforce personnel to this scheme and actively monitor accounts for unauthorized access, modification, and anomalous activities.
- Continue to educate employees on scrutinizing links contained in e-mails, and not opening attachments included in unsolicited e-mails.
- Ensure employees are aware of social engineering and phishing attacks (i.e., via phone or e-mail) by cyber criminals attempting to obtain user credentials.
- Instruct employees to refrain from providing log-in credentials or PII in response to any e-mail or phone call.
- Direct employees to report any suspicious requests for personal information to the Information Technology or Information Security Department.
- Establish company policies to contact the owner of the account to verify any changes to existing account information. Apply heightened scrutiny to bank information initiated by account holders seeking to update or change direct deposit credentials.
- Establish multi-factor authentication for creating new online accounts and for making account changes, such as password or bank account information.

# MERS Cybercrime Defenses

Constant battle  
to balance  
**Operations vs  
Security...**



...so we don't  
become the **Denial  
of Service** we are  
trying to prevent

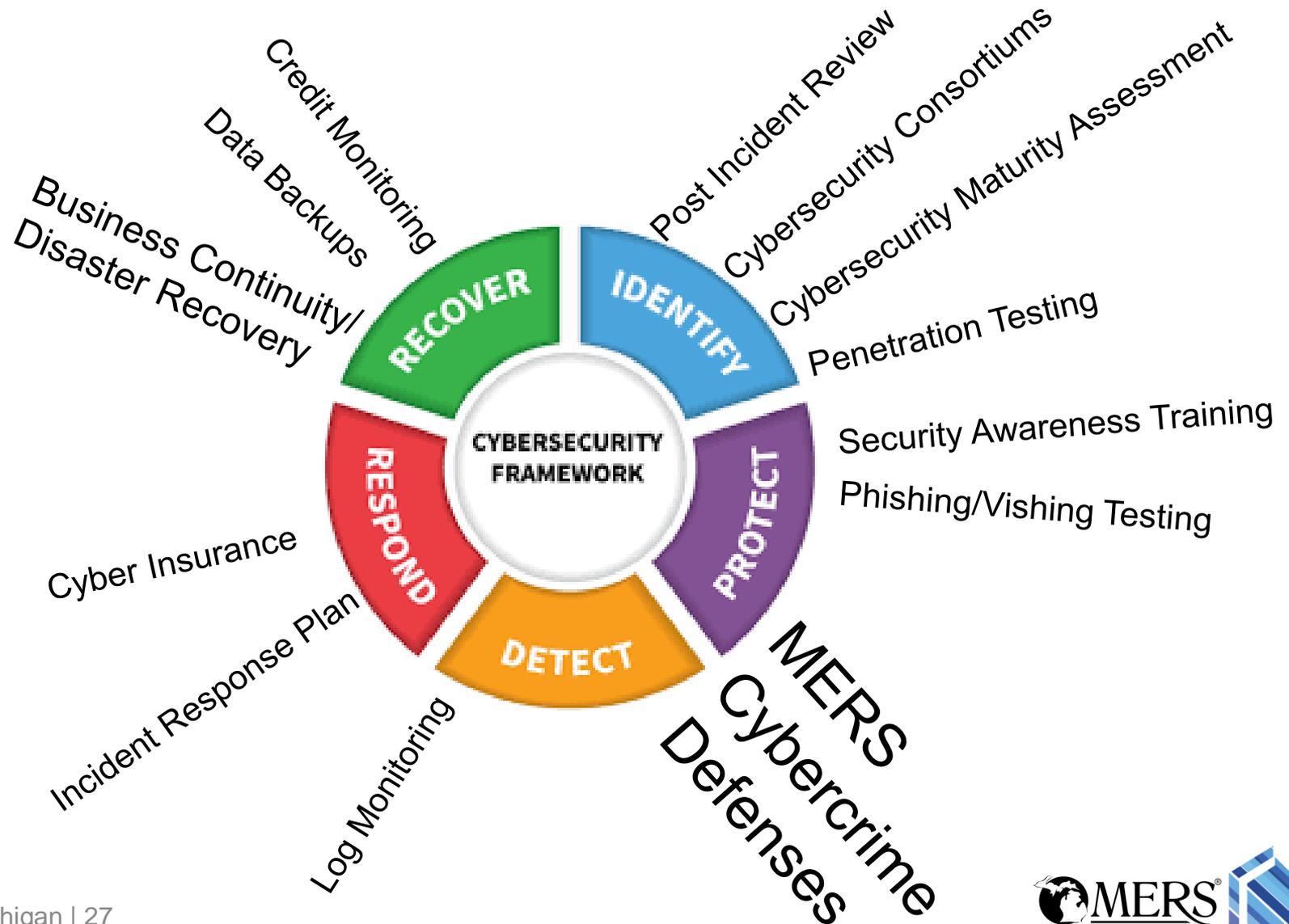
## Familiar Defenses

- Anti-Virus software (AV)
- Vulnerability scanning software
- Password Management Software
- Mobile Device Management Software
- Security Awareness Training

## Less Familiar Defenses

- Intrusion Prevention Software (IPS)
- Data Loss Prevention Software (DLP)
- 2FA Access Control for Admin Levels
- Non-Persistent Virtual Desktops
- Media Access Control (MAC) Filtering

# Cyber Incident Response

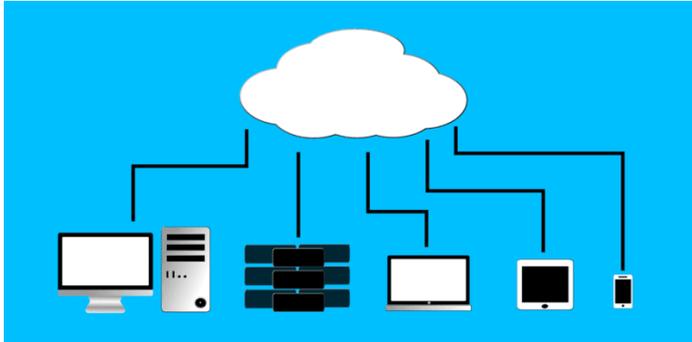


# Cybersecurity Information Sharing

- Public/private sector collaborations
- Confidential security information sharing
- Formed to combat “Black Hat” information sharing
- Dozens of emails/warnings per day (~7000/year)
- Requires FBI background check
- May require \$\$ or in-kind contribution in exchange for training



# Future Threat Landscape



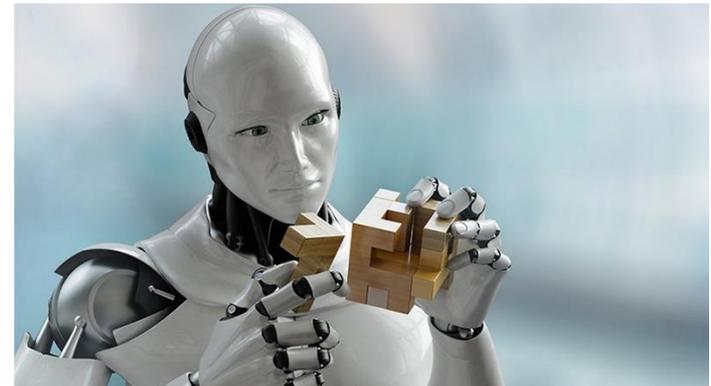
**Cloud Migrations / Solutions**



**Bot Technology**



**Internet of Things (IoT)**



**Artificial Intelligence (AI)**

# AI – Scary Possibilities...

## A Style-Based Generator Architecture for Generative Adversarial Networks

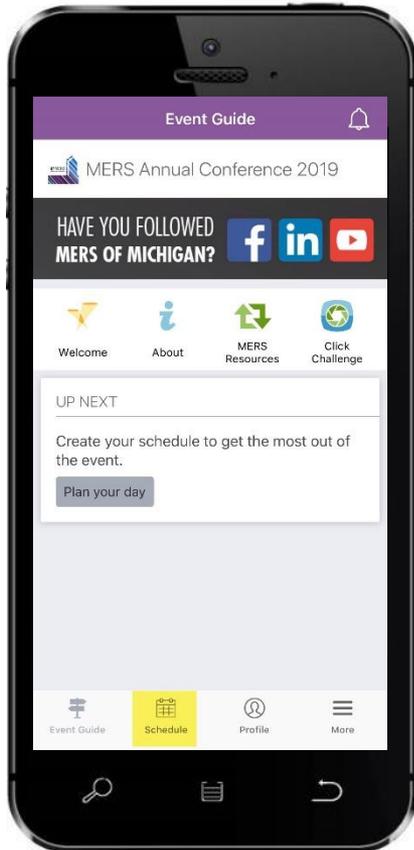
Tero Karras, Samuli Laine, Timo Aila

NVIDIA Corporation



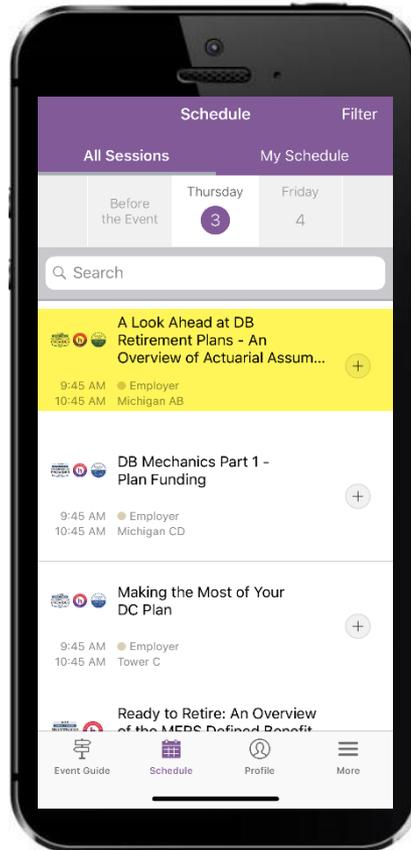
# Q & A

# Please Complete a Session Survey!



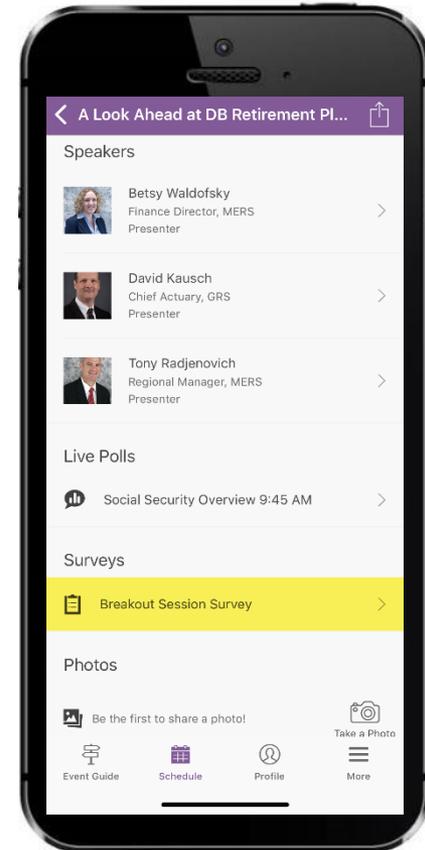
## Step 1:

Locate and access the  
"Schedule" Icon



## Step 2:

Select the **session** you  
just attended (look for  
correct date and time)



## Step 3:

Scroll down and click  
"Breakout Session  
Survey" to complete  
the survey

# Contacting MERS of Michigan

---

## MUNICIPAL EMPLOYEES' RETIREMENT SYSTEM

1134 Municipal Way  
Lansing, MI 48917

800.767.MERS (6377)

[www.mersofmich.com](http://www.mersofmich.com)



*This presentation contains a summary description of MERS benefits, policies or procedures. MERS has made every effort to ensure that the information provided is accurate and up to date. Where the publication conflicts with the relevant Plan Document, the Plan Document controls.*