Infogressive, Inc.
Cybersecurity Solved.

# OKLAHOMA'S ELECTRIC COOPERATIVES

September 2019

# Ron Batterton

## Security Account Manager

- 27 years in IT *(10 as ISO)*
- Experience In
  - Security Operations
  - Software Implementation
  - Client Support Management
  - Data Center Security (PCI)
  - Banking Operations

- University of Nebraska
  - Bachelor's in Business Finance
- CISSP, NSE3
- Interests:
  - Private Pilot, Photography, Boating, Scuba Diving, 2 College age Daughters

# AGENDA

- Talk about a few of the most recent Data Breaches –
- See what we know about them – what we don’t etc.
- Talk about some things we all need to be doing to keep up with the attackers

# LookBack Malware Targets the United States Utilities Sector with Phishing Attacks Impersonating Engineering Licensing Boards

AUGUST 01, 2019 | MICHAEL RAGGI AND DENNIS SCHWARZ WITH THE PROOFPOINT THREAT INSIGHT TEAM

## Overview

Between July 19 and July 25, 2019, several spear phishing emails were identified targeting three US companies in the utilities sector. The phishing emails appeared to impersonate a US-based engineering licensing board with emails originating from what appears to be an actor-controlled domain, nceess[.]com. Nceess[.]com is believed to be an impersonation of a domain owned by the US National Council of Examiners for Engineering and Surveying. The emails contain a malicious Microsoft Word attachment that uses macros to install and run malware that Proofpoint researchers have dubbed "LookBack." This malware consists of a remote access Trojan (RAT) module and a proxy mechanism used for command and control (C&C) communication. We believe this may be the work of a state-sponsored APT actor based on overlaps with historical campaigns and macros utilized. The utilization of this distinct delivery methodology coupled with unique LookBack malware highlights the continuing threats posed by sophisticated adversaries to utilities systems and critical infrastructure providers.

HEALTH IT SECURITY

xtelligent HEALTHCARE MEDIA

**Monday This week:**

- 5 Providers Report Patient Breaches due to Phishing Attacks
- Includes East Central Indiana School Trust and the University of Cincinnati Health
- https://healthitsecurity.com/

# WHY THE PROBLEM EXITS

The technology is complex and expensive

The hackers and their tools/tech quickly evolve

0% unemployment rate for cybersecurity engineers

Lack of understanding and awareness

# THE SOLUTION

Our defense in depth approach gives you a 360-degree platform that makes it easy to worry less about the security of your company's data and focus more on your business.

# CYBER CRIME STATISTICS


America
is #1

SMB's are target
43% of the time

Ransomware
occurs every
14 seconds

# Current Cybersecurity Program


NAILED IT.

# CIS 20 CRITICAL CONTROLS

## What is it?

A prioritized list of security controls that secure your entire organization against today's most pervasive threats.

## Why are they important?

It works. Organizations that do the CIS Controls well - can eliminate the vast majority of an organization's vulnerabilities.

# SANS CIS 20 CRITICAL CONTROLS:

## Basic CIS Controls

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

## Foundational CIS Controls

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

## Organizational CIS Controls

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

76%

of businesses have experienced a phishing attack

45%

have experienced phishing via a phone call or text message


Lock Picking 101

Phishing was the #1 threat action used in successful breaches linked to social engineering and malware attacks.

*Verizon's 2019 Data Breach Investigation Report*

# 2019 Phishing by Industry Benchmarking Report: Methodology and Data Set

| 19 | 18k | 9M | 20M | 3 |
|---|---|---|---|---|
| Industries | Organizations in three size ranges – 1-249, 250-999, 1000+ | Unique recipients included in the Baseline Phishing Security Test | Phishing Security Tests over 12 months | Phases of testing |

Phase

# 1

| Industry | 1-249 Emp | 250-999 Emp | 1000+ Emp |
|---|---|---|---|
| Banking | 29.3 | 31.3 | 25.7 |
| Business Services | 34.5 | 31.7 | 27.9 |
| Construction | 37.9 | 37.1 | 36.7 |
| Consulting | 29.2 | 31.9 | 24.2 |
| Consumer Services | 36.3 | 33.3 | 23 |
| Education | 33.6 | 31.4 | 28.2 |
| Energy & Utilities | 34.8 | 32 | 34.4 |
| Financial Services | 31.1 | 31.7 | 29.1 |
| Government | 34.7 | 29.8 | 23.5 |
| Healthcare & Pharmaceuticals | 33.1 | 32.9 | 27.6 |
| Hospitality | 34 | 23.6 | 48.4 |
| Insurance | 36.4 | 34.9 | 31.2 |
| Legal | 32.2 | 29.6 | 32.7 |
| Manufacturing | 36.1 | 34.1 | 30.9 |
| Not-For-Profit | 35.4 | 32.3 | 30.1 |
| Other | 31 | 29.2 | 22.4 |
| Retail & Wholesale | 36.7 | 32.9 | 26.4 |
| Technology | 34.3 | 31.3 | 31.4 |
| Transportation | 33.5 | 33.7 | 16.4 |

## Baseline Phish-prone Percentage by Industry

**30%***

Initial Baseline PPP across all industries and sizes

| Org Size | Initial PPP |
|---|---|
| 1-249 | 33.5 |
| 250-999 | 31.9 |
| 1000+ | 27.9 |

*Percentage rounded

*Computer-based training is defined as the delivery of standardized sets of interactive education and/or behavior management content to users via a laptop, desktop, or tablet.*

Phase

# 2

| Industry | 1-249 Emp | 250-999 Emp | 1000+ Emp |
|---|---|---|---|
| Banking | 9.7 | 12 | 16.4 |
| Business Services | 15.9 | 13.3 | 21.3 |
| Construction | 16.8 | 19.7 | 15 |
| Consulting | 13 | 13.7 | 4.1 |
| Consumer Services | 16.1 | 16.5 | 15.4 |
| Education | 18.6 | 20.9 | 19.3 |
| Energy & Utilities | 13.9 | 16 | 13 |
| Financial Services | 12.6 | 13.2 | 16.4 |
| Government | 14.5 | 14.9 | 10.8 |
| Healthcare & Pharmaceuticals | 17.8 | 14.8 | 19 |
| Hospitality | 26.5 | 14.3 | 0* |
| Insurance | 15.5 | 16 | 15.3 |
| Legal | 15.6 | 11.4 | 3.8 |
| Manufacturing | 16.5 | 15.9 | 14.6 |
| Not-For-Profit | 16.3 | 16.5 | 16.4 |
| Other | 16.3 | 19.7 | 13.7 |
| Retail & Wholesale | 15.6 | 13.3 | 15.8 |
| Technology | 16.9 | 16.9 | 17.2 |
| Transportation | 12.1 | 19.6 | 15.8 |

*Data set too low*

## Results after 90 Days of CBT & Phishing Testing

# 15%*

90 Day % PPP across all industries and sizes

| Org Size | Initial PPP |
|---|---|
| 1-249 | 14.7 |
| 250-999 | 15.9 |
| 1000+ | 15.9 |

*Percentage rounded*

Phase

# 3

| Industry | 1-249 Emp | 250-999 Emp | 1000+ Emp |
|---|---|---|---|
| Banking | 1.3 | 1.9 | 3.2 |
| Business Services | 1.7 | 2 | 3.2 |
| Construction | 1.8 | 3.1 | 7.9 |
| Consulting | 1.8 | 2 | 0.8 |
| Consumer Services | 1.7 | 2.5 | 2.8 |
| Education | 2.69 | 2.3 | 4.3 |
| Energy & Utilities | 2.2 | 1.9 | 5.3 |
| Financial Services | 1.6 | 2.1 | 5.6 |
| Government | 2.1 | 2 | 2 |
| Healthcare & Pharmaceuticals | 1.7 | 1.9 | 3.5 |
| Hospitality | 1 | 2.5 | 0* |
| Insurance | 2.2 | 2.9 | 4.5 |
| Legal | 2.3 | 3.4 | 2.3 |
| Manufacturing | 2.5 | 2 | 2 |
| Not-For-Profit | 2.2 | 2 | 2.6 |
| Other | 1.9 | 2.2 | 1.4 |
| Retail & Wholesale | 1.8 | 2.4 | 4 |
| Technology | 2.1 | 2.2 | 2.7 |
| Transportation | 1 | 4.9 | 1.2 |

*Data set too low*

## Results after 1 Year of CBT & Phishing Testing

# 2%*

One Year % PPP across all industries and sizes

| Org Size | Initial PPP |
|---|---|
| 1-249 | 1.9 |
| 250-999 | 2.2 |
| 1000+ | 3 |

*Percentage rounded*

# Plan Like a Leader – We're trying to improve behaviors!
# Test Like an Attacker – Make it Real

- Use Real World Attack Methods
- Don't Do it Alone
- Don't Try to Train on Everything
- Make it Relevant
- Treat the Program like a Marketing Campaign

Infogressive

Our defense in depth approach maps to 15 of the CIS 20 Critical Controls

# PERIMETER SECURITY

The days of set it & forget it no longer exist

6 Controls


- #7 – Email & Web Browser Protection
  - 7.4 (Network-based URL Filters), 7.5 – 7.6 (URL categorization & Logging), 7.7 (DNS Filtering)
- #9 – Limit/Control of Network Ports, Protocols
  - 9.2 (Ensure only approved Ports, Protocols, and Services are running), 9.5 (Implement Application Firewalls)

#11 – Secure Configuration of Network Devices

- 11.1 (Maintain Standard Security Configs), 11.2 (Document Traffic Config Rules), 11.4 (Install Latest Version of Security Updates on all Network Devices), 11.5 (Manage Network Devices using MFA & Encrypted Sessions), 11.7 (Manage Network Infrastructure Through Dedicated Network)

*Continued…*

# PERIMETER SECURITY

The days of set it & forget it no longer exist

6
Controls


- #12 – Boundary Defense
  - 12.1 (Maintain an Inventory of Network Boundaries), 12.2 (Scan for Unauth. Connections), 12.3 (Deny Communications with Malicious IPs), 12.4 (Deny Communication over Unauth. Ports), 12.6 (Deploy Network-Based IDS Sensors), 12.7 (Deploy Netowork-Based IPS), 12.9 (Deploy App-layer Filtering Proxy Server), 12.10 (Decrypt Network Traffic at Proxy), 12.11 (Require MFA for All Remote Logins), 12.12 (Manage All Devices Remotely Logging into Internal Network)
- #13 – Data Protection
  - 13.3 (Monitor & Block Unauth. Network Traffic)
- #14 – Controlled Access
  - 14.1 – 14.2 (Network Segmentation & FW Filtering)

# EMAIL SECURITY

91% of breaches begin with a malicious email

3 Controls


- #7 – Email & Web Protections
  - 7.8 (Anti-Spoofing with DMARC, SPF, or DKIM), 7.9 (Block Unnecessary File Types in Emails), 7.10 (Sandbox All Email Attachments)
- #14 – Controlled Access
  - 14.4 (Encrypt Data In-Transit)
- #17 – Security Awareness Training Program
  - Our Phishing & Security Awareness Training Service covers Control 17 and helps increase employee security knowledge & competency

# VULNERABILITY MANAGEMENT

3 Controls

Move your team from reactive to proactive


- #1 – Inventory & Control of Hardware Assets
  - 1.1 (Active Discovery), 1.6 (Address Unauth. Assets)
- #3 – Continuous Vulnerability Management
  - 3.1 – 3.3 (Run Scans w/ Automated Vuln Scanning Tools), 3.6 – 3.7 (Compare Scans, Utilize Risk-Ratings)
- #18 – Application Software Security
  - 18.7 – 18.8 (Establish a Process to Analyze & Report Web App Security & Vulnerabilities)

# ENDPOINT SECURITY

97% of malware is unique to a specific endpoint

2 Controls


- #8 – Malware Defenses
  - 8.1 – 8.2 (Centrally Managed AV installed & kept up-to-date), 8.6 (Centralize AV Logging)
- #13 – Data Protection
  - 13.6 – 13.7 (Monitor & Manage Device Encryption)

# MDR (MANAGED DETECTION & RESPONSE)

## Combining people & technology to find attackers

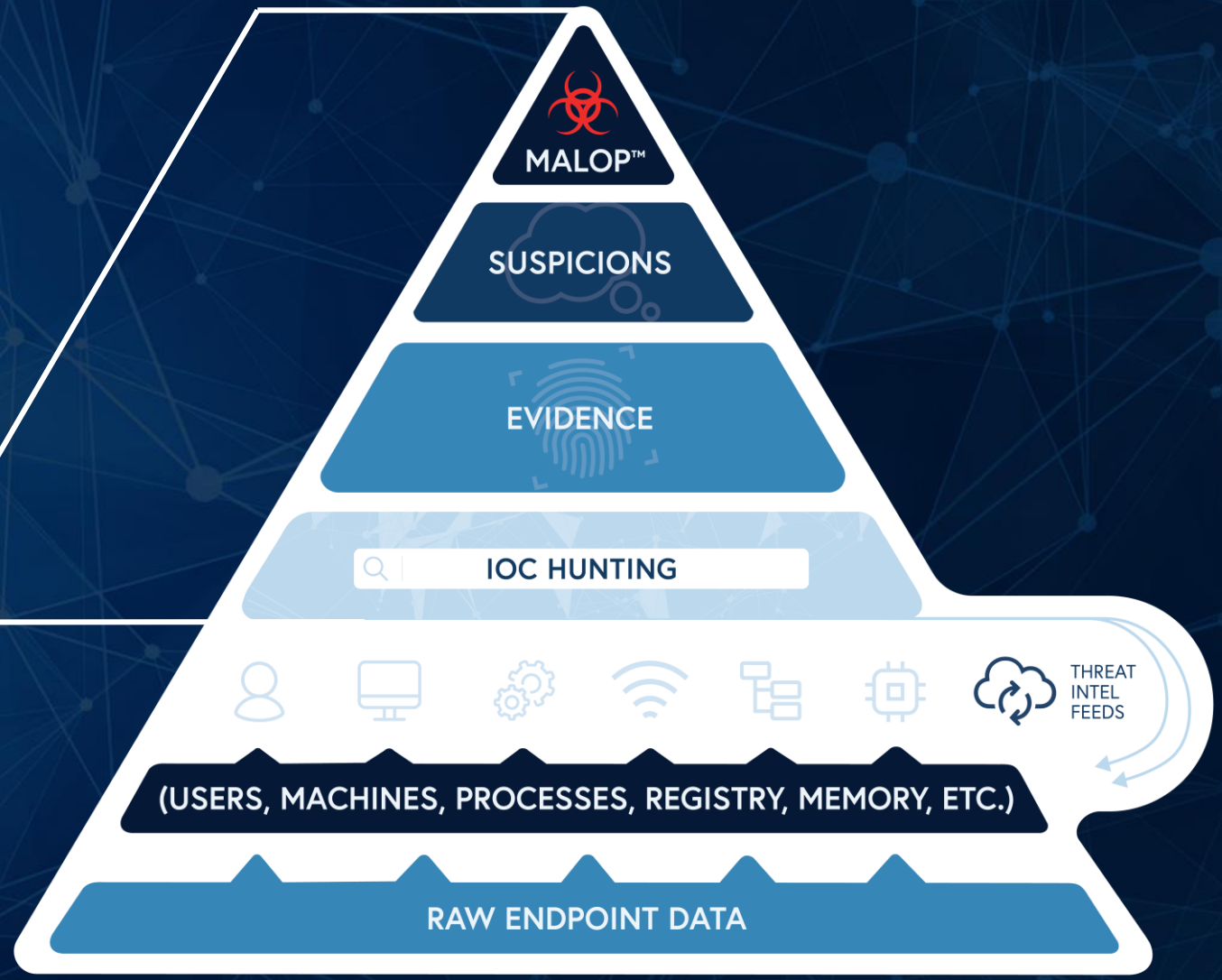
4
Controls


- #4 – Controlled Use of Admin Privileges
  - 4.8 – 4.9 (Log & Alert on Admin Account Changes, Admin Group Membership, & Unsuccessful Logins)
- #6 – Maintenance, Monitoring, & Analysis of Logs
  - Our Log Analysis service covers this control entirely
- #8 – Malware Defenses
  - 8.8 (Audit/Monitor Malicious Use of Command Line)
- #16 – Account Monitoring & Control
  - 16.12 - 16.13 (Monitor & Alert on Unusual Account Login Behaviors/Activity)

# Behavioral Detection & Response Powered by Analytics (EDR)

**8M**

questions per second



# STAYING AHEAD OF THE ATTACK

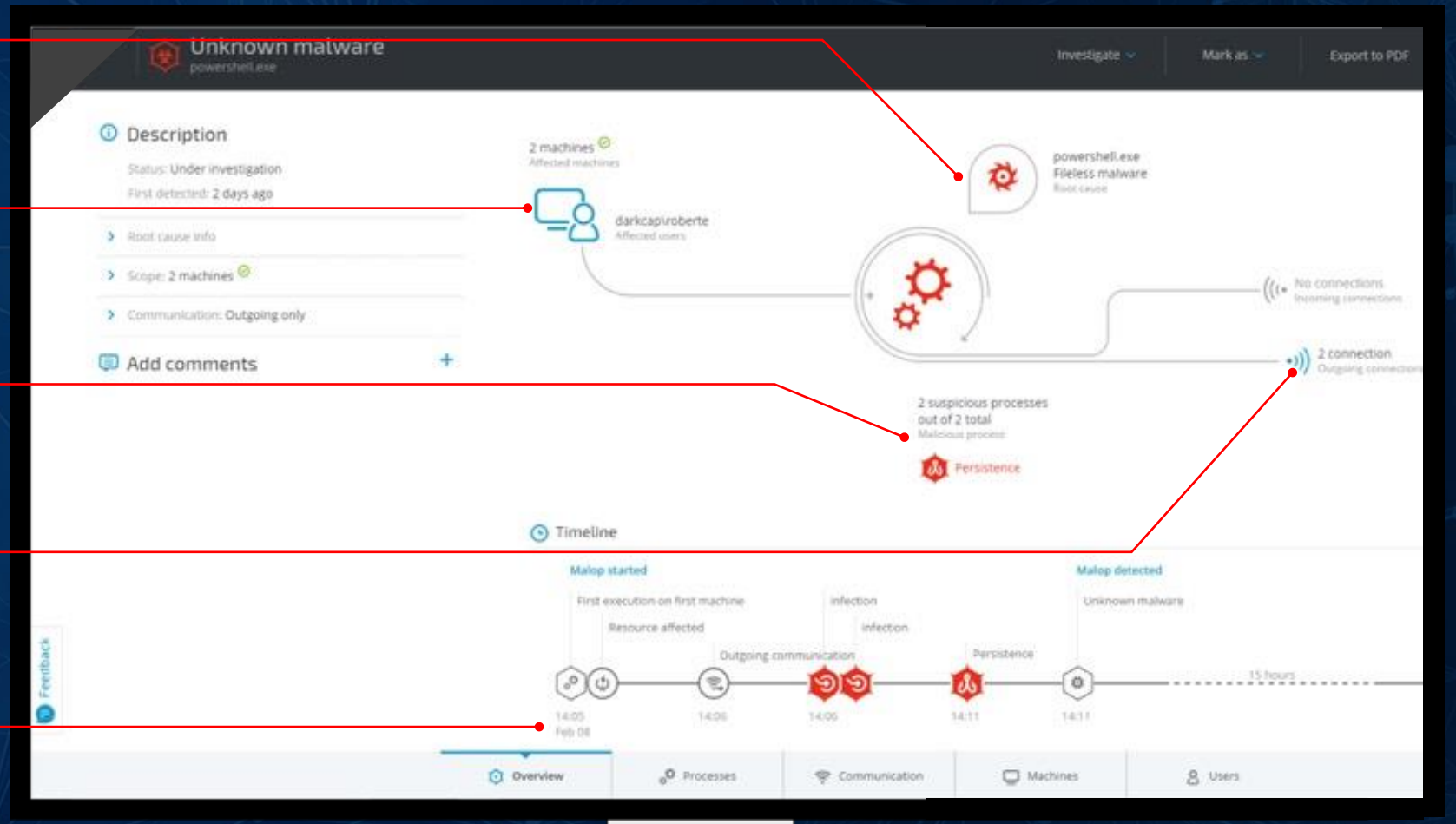
Determine the root cause

Find affected users and machines

Learn which tools were used

Analyze attacker communications

Create the timeline of attack



# PROFESSIONAL SERVICES

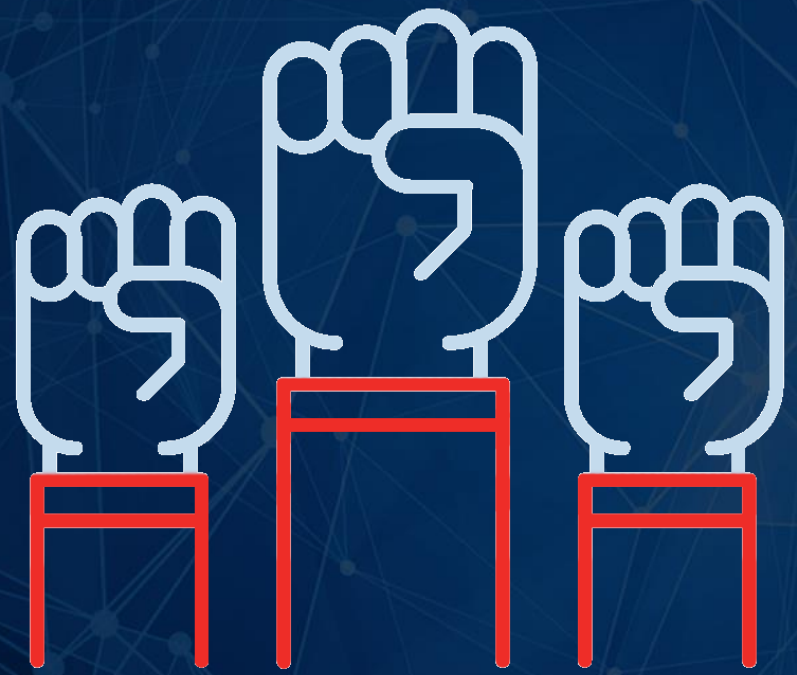
## Our security experts play offense & defense

3
Controls


- Penetration Testing
  - #20 – Penetration Testing & Red Team Exercises
- Risk Assessments
  - CIS 20 Holistically
- Incident Response
  - #19 – Incident Response & Management:

    *Our IR service can be integrated into your Incident Response & Management plan.*

# THE MOST IMPORTANT QUESTIONS



Do you have support from your organization?

Do you have a budget?

“Of course, money alone is not the answer — as we found in the study, higher cybersecurity spending doesn’t necessarily translate into a higher cybersecurity maturity level,” “While everyone is looking for an efficiency ratio for their cyber costs, how a security program is planned, executed and governed is as important, if not more.”

- Julie Bernard, a principal with Deloitte Risk and Financial Advisory’s cyber risk services, Deloitte & Touche LLP.

67% increase in security breaches
over the last 5 years

Last year Cybercrime
profited over $1.5 Trillion

That number is expected to
reach over $6 Trillion by 2021

Questions & Discussion

# Thank You

Ron Batterton (402) 261-0123 x112
ron.batterton@Infogressive.com
**Infogressive.com**