Nonprofit Cybersecurity Incident Report

Community IT Innovators®

TechForward #Secured

September 2019

About Community IT

100% Employee Owned

Advancing mission through the effective use of technology.

Channel Futures™

MSP 501

2019 WINNER

Presenter

Matthew Eshleman
CTO

NONPROFIT CYBERSECURITY INCIDENT REPORT

February 2019 1st Edition

Agenda

Cybersecurity landscape

Our approach to cybersecurity

Types of incidents

Report data

Engage your leadership

Secure your organization

CYBERSECURITY LANDSCAPE

Persistent and ongoing brute force attacks on identities

Sophisticated spear phishing

Organizations targeted because of the work they do

Attacks targeting vendors

CYBERSECURITY LANDSCAPE

New security tools available to combat new threat types.

Organization’s starting to ask about where to start in improving their cybersecurity.

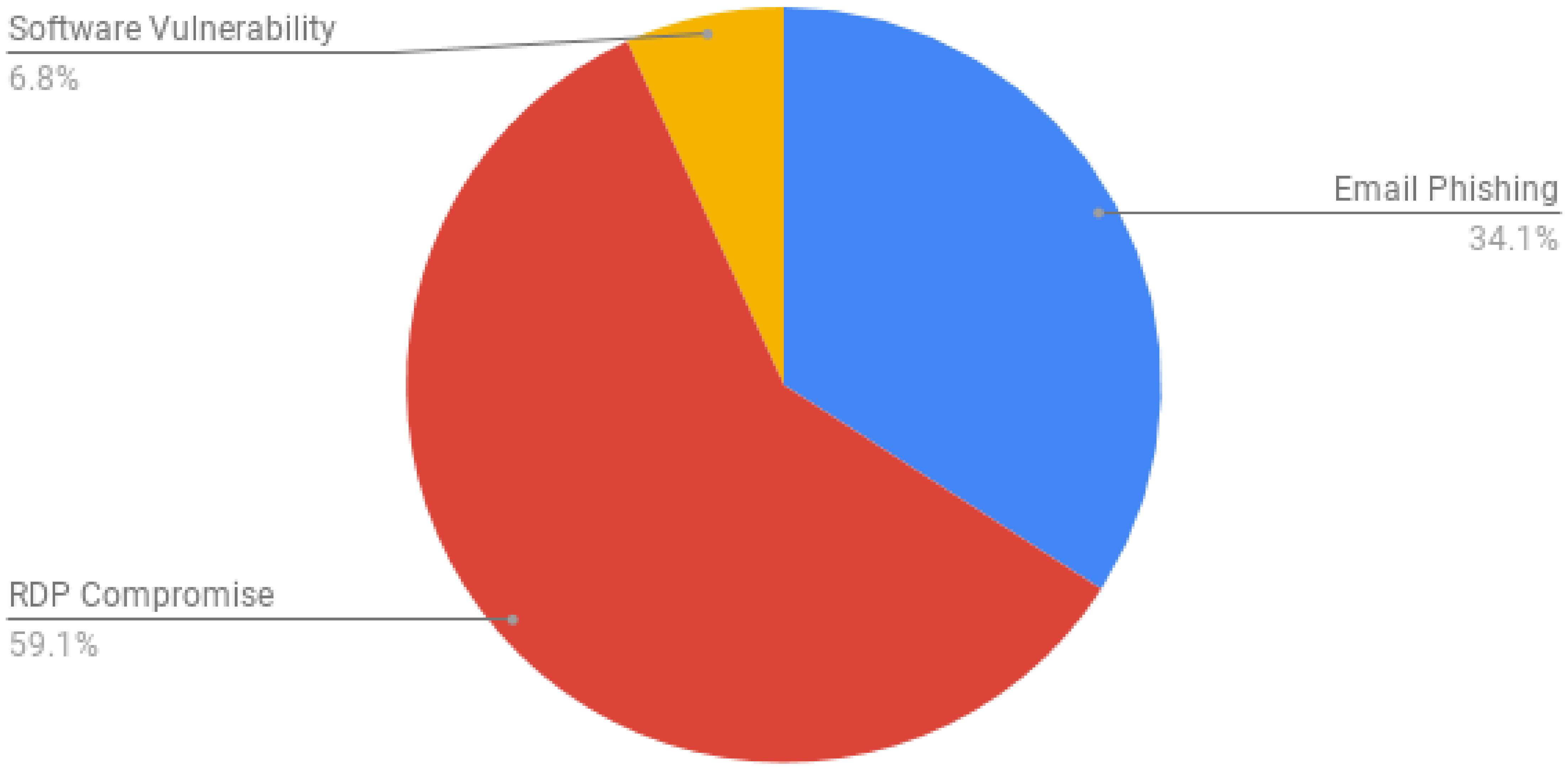
68% of Nonprofits don’t have an Incident Response Plan

Breach response for a small to medium business is $149,000

Cybersecurity - Adversaries

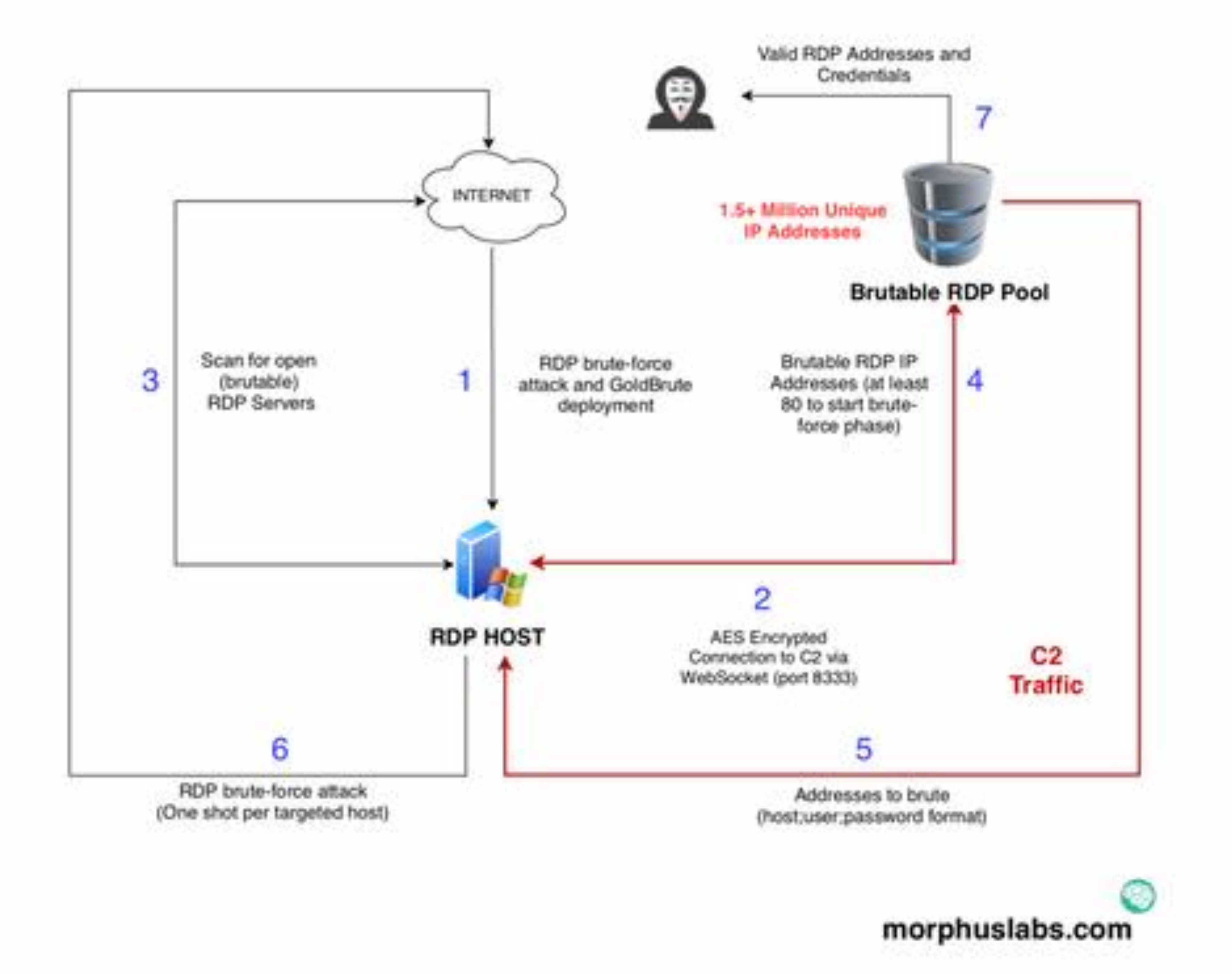
Cybersecurity Landscape

Attack Vectors Commonly Used in Ransomware Incidents: Q2 2019

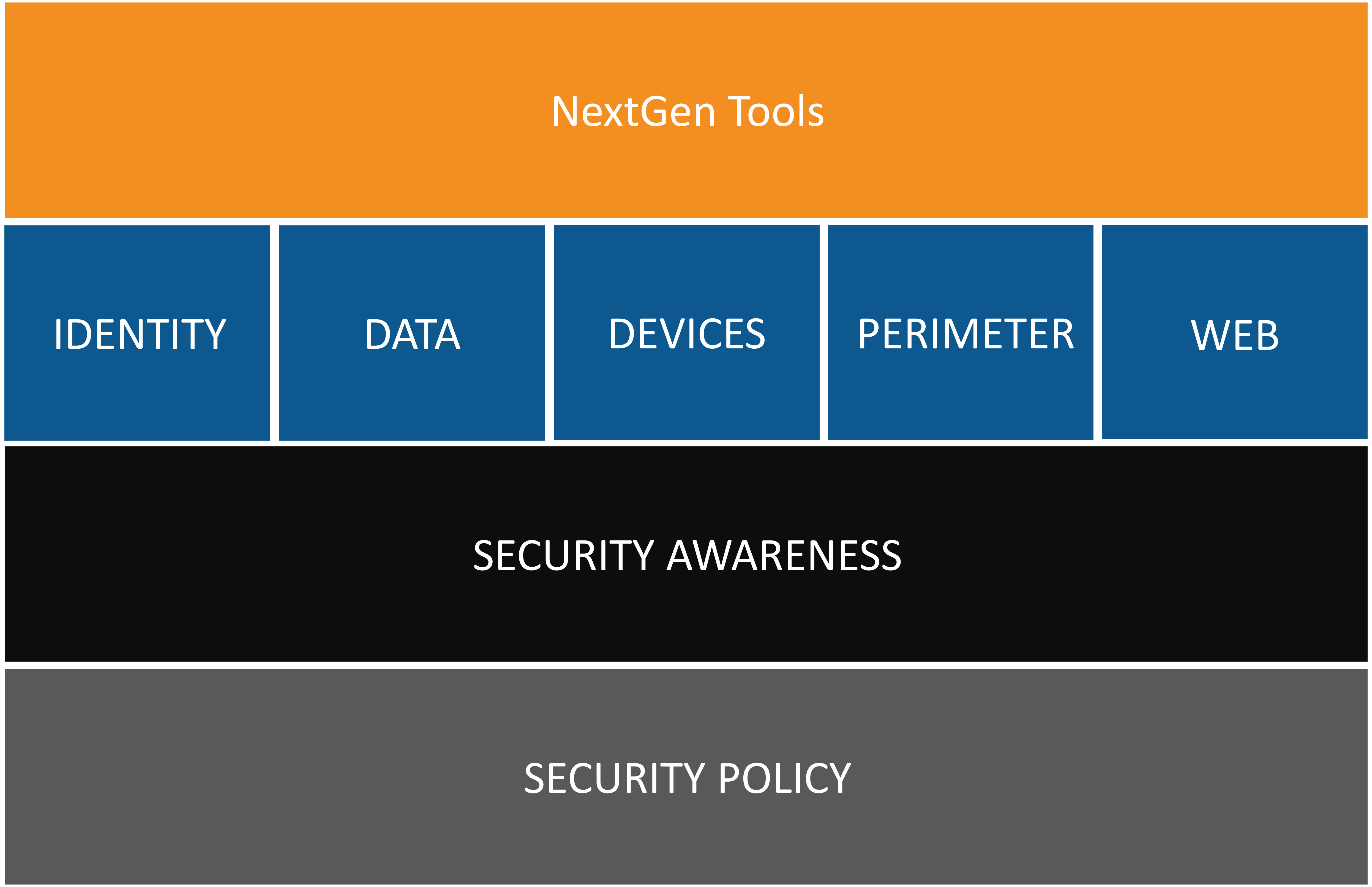


https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread

1.5 Million RDP Servers Attacked


Valid RDP Addresses and Credentials
7
INTERNET
1.5+ Million Unique IP Addresses
Brutable RDP Pool
3
Scan for open (brutable) RDP Servers
1
RDP brute-force attack and GoldBrute deployment
Brutable RDP IP Addresses (at least 80 to start brute-force phase)
4
RDP HOST
2
AES Encrypted Connection to C2 via WebSocket (port 8333)
C2 Traffic
6
RDP brute-force attack (One shot per targeted host)
5
Addresses to brute (host;user;password format)
morphuslabs.com

OUR APPROACH TO CYBERSECURITY



NextGen Tools

IDENTITY

DATA

DEVICES

PERIMETER

WEB

SECURITY AWARENESS

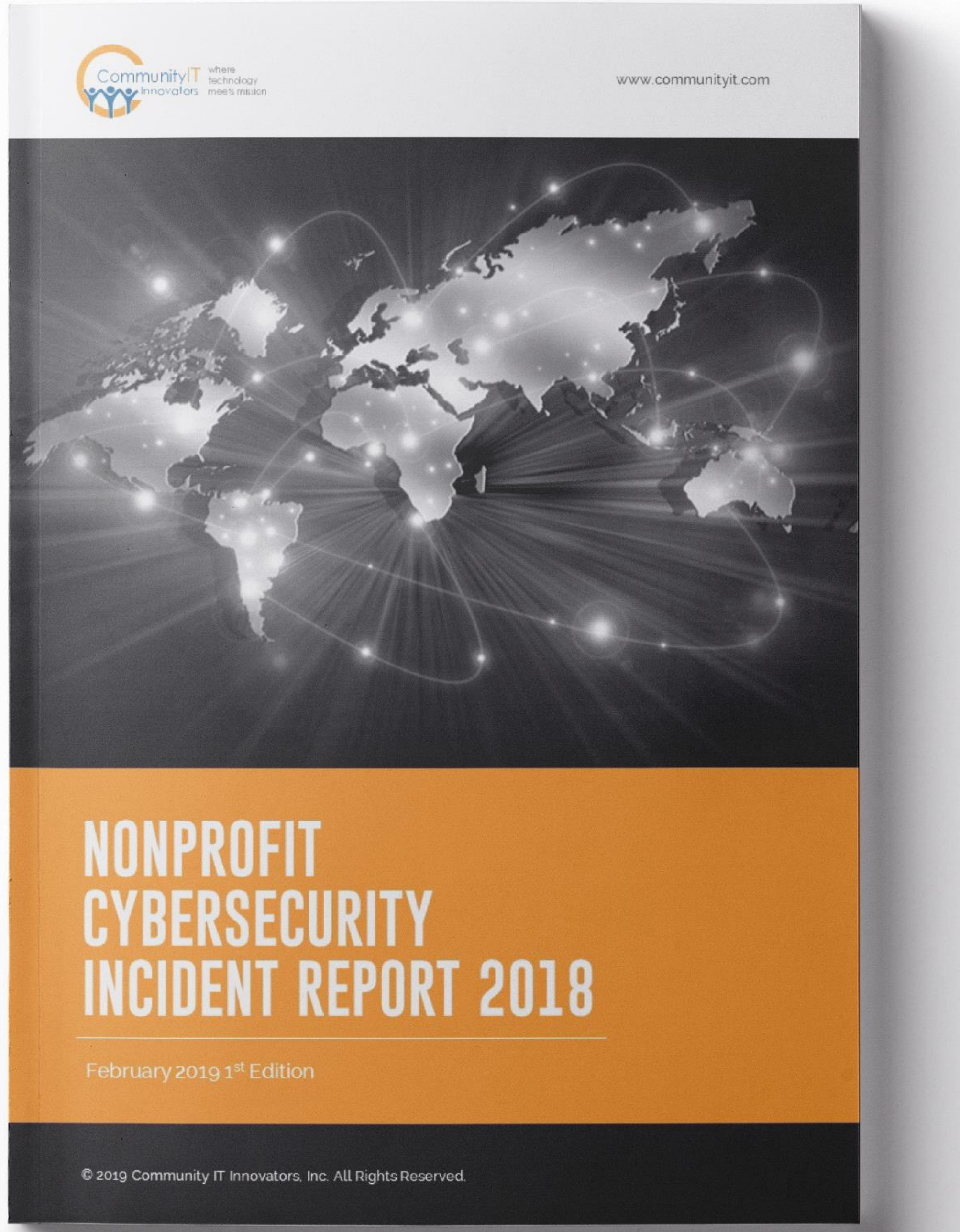
SECURITY POLICY

Incident

An event that compromises the integrity, confidentiality or availability of an information asset.

Breach

An incident that results in the confirmed disclosure—
not just potential exposure—of data to an unauthorized party.

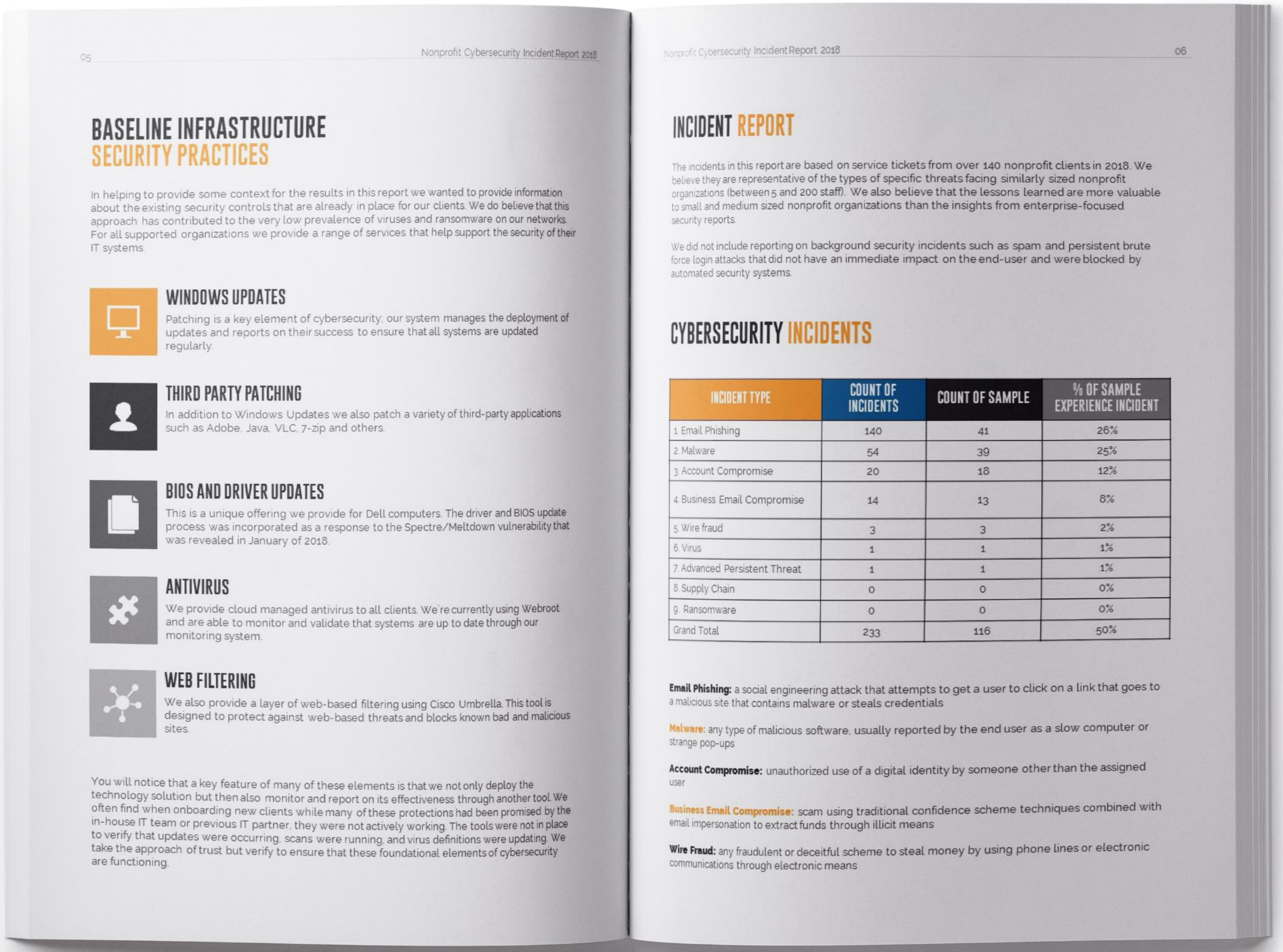


CommunityIT Innovators where technology meets mission

www.communityit.com

NONPROFIT CYBERSECURITY INCIDENT REPORT 2018

February 2019 1st Edition



05 Nonprofit Cybersecurity Incident Report 2018

BASELINE INFRASTRUCTURE SECURITY PRACTICES

In helping to provide some context for the results in this report we wanted to provide information about the existing security controls that are already in place for our clients. We do believe that this approach has contributed to the very low prevalence of viruses and ransomware on our networks. For all supported organizations we provide a range of services that help support the security of their IT systems.

WINDOWS UPDATES

Patching is a key element of cybersecurity; our system manages the deployment of updates and reports on their success to ensure that all systems are updated regularly.

THIRD PARTY PATCHING

In addition to Windows Updates we also patch a variety of third-party applications such as Adobe, Java, VLC, 7-zip and others.

BIOS AND DRIVER UPDATES

This is a unique offering we provide for Dell computers. The driver and BIOS update process was incorporated as a response to the Spectre/Meltdown vulnerability that was revealed in January of 2018.

ANTIVIRUS

We provide cloud managed antivirus to all clients. We're currently using Webroot and are able to monitor and validate that systems are up to date through our monitoring system.

WEB FILTERING

We also provide a layer of web-based filtering using Cisco Umbrella. This tool is designed to protect against web-based threats and blocks known bad and malicious sites.

You will notice that a key feature of many of these elements is that we not only deploy the technology solution but then also monitor and report on its effectiveness through another tool. We often find when onboarding new clients while many of these protections had been promised by the in-house IT team or previous IT partner, they were not actively working. The tools were not in place to verify that updates were occurring, scans were running, and virus definitions were updating. We take the approach of trust but verify to ensure that these foundational elements of cybersecurity are functioning.

Nonprofit Cybersecurity Incident Report 2018 06

INCIDENT REPORT

The incidents in this report are based on service tickets from over 140 nonprofit clients in 2018. We believe they are representative of the types of specific threats facing similarly sized nonprofit organizations (between 5 and 200 staff). We also believe that the lessons learned are more valuable to small and medium sized nonprofit organizations than the insights from enterprise-focused security reports.

We did not include reporting on background security incidents such as spam and persistent brute force login attacks that did not have an immediate impact on the end-user and were blocked by automated security systems.

CYBERSECURITY INCIDENTS

INCIDENT TYPE	COUNT OF INCIDENTS	COUNT OF SAMPLE	% OF SAMPLE EXPERIENCE INCIDENT
1. Email Phishing	140	41	26%
2. Malware	54	39	25%
3. Account Compromise	20	18	12%
4. Business Email Compromise	14	13	8%
5. Wire fraud	3	3	2%
6. Virus	1	1	1%
7. Advanced Persistent Threat	1	1	1%
8. Supply Chain	0	0	0%
9. Ransomware	0	0	0%
Grand Total	233	116	50%

Email Phishing: a social engineering attack that attempts to get a user to click on a link that goes to a malicious site that contains malware or steals credentials

Malware: any type of malicious software, usually reported by the end user as a slow computer or strange pop-ups

Account Compromise: unauthorized use of a digital identity by someone other than the assigned user

Business Email Compromise: scam using traditional confidence scheme techniques combined with email impersonation to extract funds through illicit means

Wire Fraud: any fraudulent or deceitful scheme to steal money by using phone lines or electronic communications through electronic means

Types of incidents

- **Email Phishing**: a social engineering attack that attempts to get a user to click on a link that goes to a malicious site that contains malware or steals credentials
- **Malware:** any type of malicious software, usually reported by the end user as a slow computer or strange pop-ups
- **Account Compromise:** unauthorized use of a digital identity by someone other than the assigned user

Types of incidents

- **Business Email Compromise**: scam using traditional confidence scheme techniques combined with email impersonation to extract funds through illicit means
- **Wire Fraud:** any fraudulent or deceitful scheme to steal money by using phone lines or electronic communications through electronic means
- **Virus**: a malicious piece of software that can alter the way a computer works, typically spread from one computer to another, often rendering the computer and/or data unusable

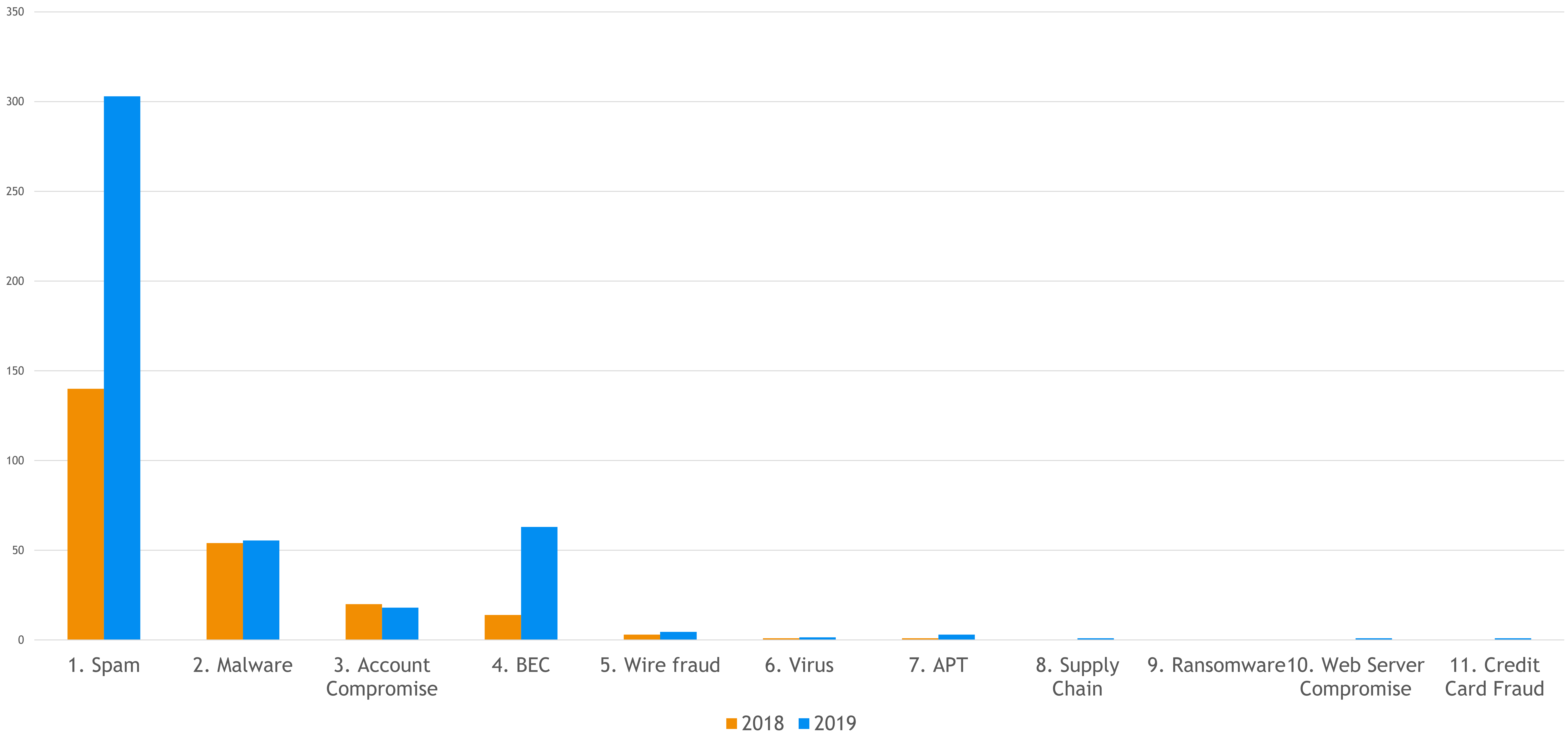
Types of incidents

- **Supply Chain:** an attack that is initiated through a partner of the organization. Also known as a value-chain or third-party attack.
- **Advanced Persistent Threat:** State-Sponsored actor or criminal group focused on targeting a specific organization or individual, operating over a long period of time with a goal of remaining undetected and exfiltrating data.
- **Ransomware:** a type of virus that has the characteristic of encrypting files and then demanding payment for decrypting the files.

CYBERSECURITY INCIDENTS - 2018

INCIDENT TYPE	COUNT OF INCIDENTS	COUNT OF SAMPLE	% OF SAMPLE EXPERIENCE INCIDENT
1. Email Phishing	140	41	26%
2. Malware	54	39	25%
3. Account Compromise	20	18	12%
4. Business Email Compromise	14	13	8%
5. Wire fraud	3	3	2%
6. Virus	1	1	1%
7. Advanced Persistent Threat	1	1	1%
8. Supply Chain	0	0	0%
9. Ransomware	0	0	0%
Grand Total	**233**	**116**	**50%**

Year to date trends



Year over Year Comparison

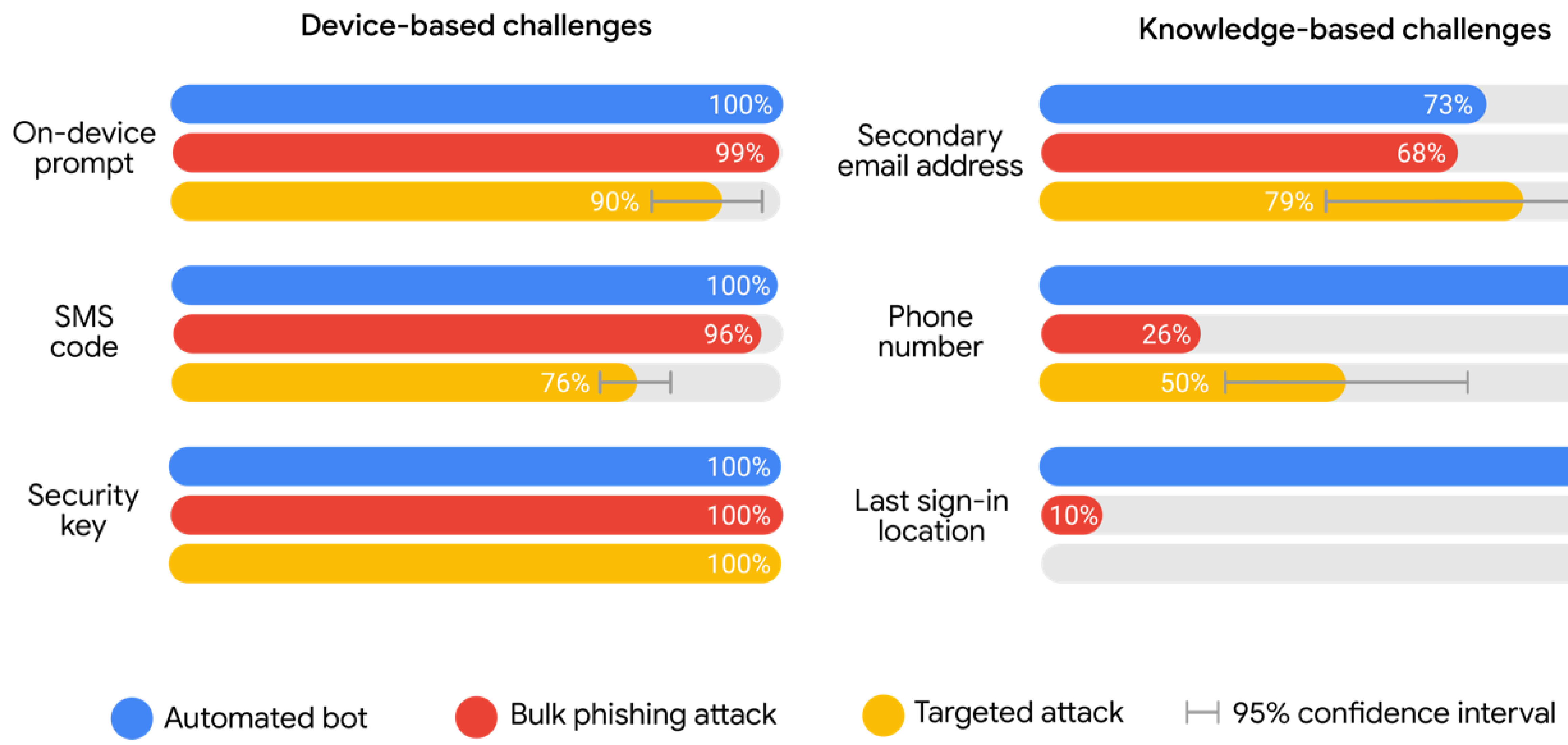
- Volume of reported spam increased
- Business Email Compromise has spiked
- Account compromises holds steady, even among increasing MFA adoption
- Wire Fraud has increased
- Actual virus infection rate is low
- Ransomware in sample is low

Analysis of Our Data and Sector

- Spearphishing / Business Email Compromise is increasing
- Supply chain attacks up dramatically in our sector
    - Vendor -> Client
    - Org -> Org
- Security Awareness Training adoption is increasing
- MFA adoption is increasing
- We still have a long way to go

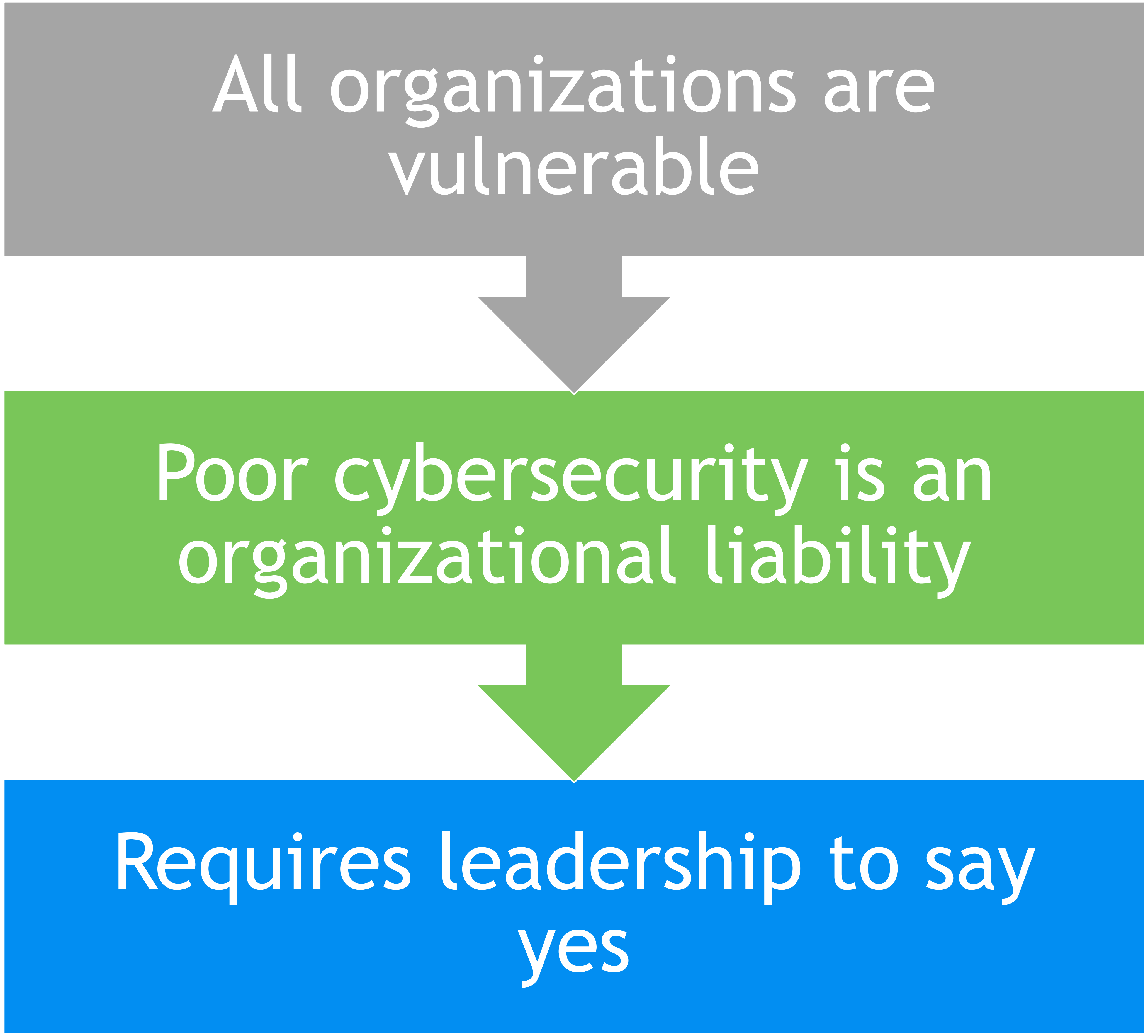
MFA is Effective

Account takeover prevention rates, by challenge type



Knowledge into Action

Engage your Leadership



All organizations are vulnerable

Poor cybersecurity is an organizational liability

Requires leadership to say yes

Engage your Leadership

Schedule

- Schedule time for cybersecurity
  - Monthly reporting
  - Quarterly planning

Know

- Know your audience
  - Narrative
  - Metrics and numbers

Leverage

- Leverage existing compliance requirements
  - PCI
  - HIPAA
  - GDPR

Cybersecurity Readiness

People

- Passwords
- MFA

Process

- Policy
- Security Awareness Training

Technology

- Antivirus
- Backup
- Email Protection
- Etc..

Getting Started with Cybersecurity

- IT Policy
- Security Awareness Training
- OS and Third Party Updates
- Antivirus
- Backups
- MultiFactor Auth
- Business Email Compromise Protection

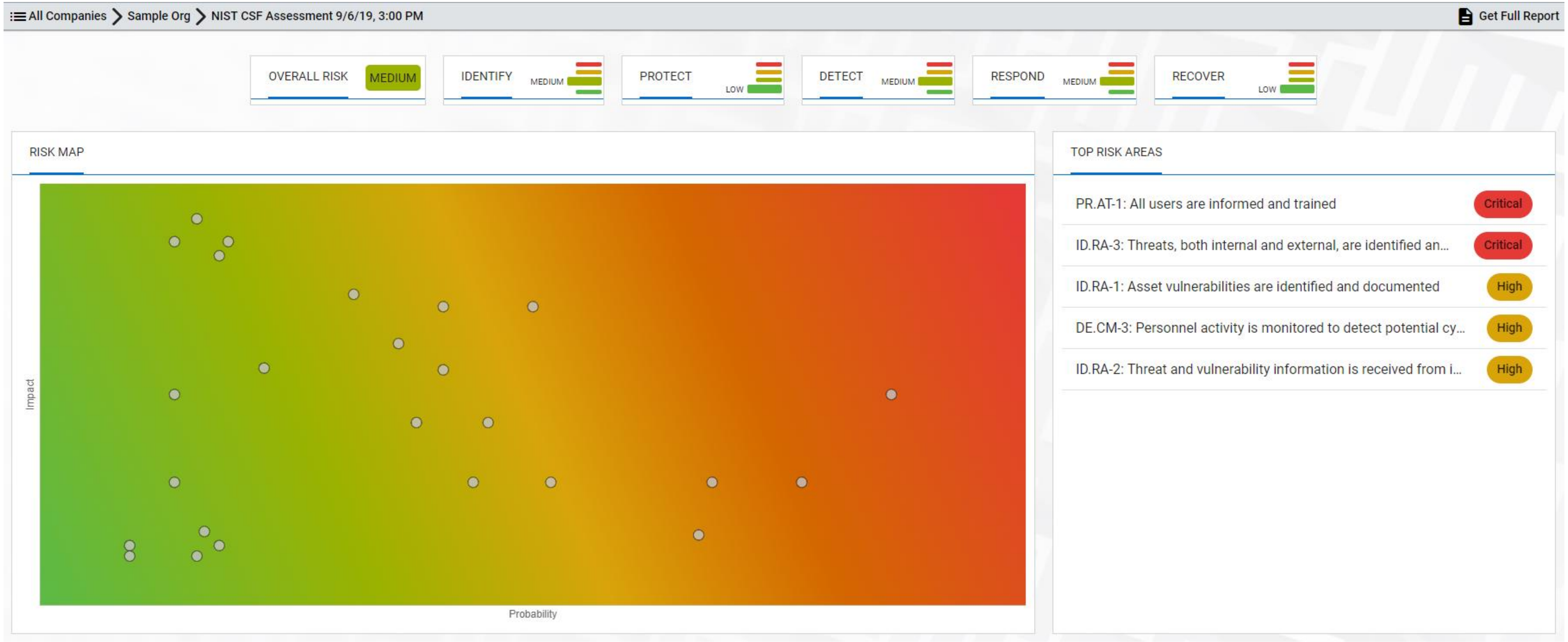
Growing Organization

- BIOS / Driver Updates
- Web Filtering
- BYOD Control
- Device Encryption
- Endpoint Detection and Response
- Risk Assessment

Mature/Compliant Organization

- Cyberliablity Insurance
- Cybersecurity Assessment
- SOC / SIEM
- Vulnerability Scanning
- Penetration Testing

NIST Risk Assessment Tool



All Companies > Sample Org > NIST CSF Assessment 9/6/19, 3:00 PM

Get Full Report

OVERALL RISK MEDIUM

IDENTIFY MEDIUM

PROTECT LOW

DETECT MEDIUM

RESPOND MEDIUM

RECOVER LOW

RISK MAP

TOP RISK AREAS

PR.AT-1: All users are informed and trained	Critical
ID.RA-3: Threats, both internal and external, are identified an...	Critical
ID.RA-1: Asset vulnerabilities are identified and documented	High
DE.CM-3: Personnel activity is monitored to detect potential cy...	High
ID.RA-2: Threat and vulnerability information is received from i...	High

Resources

- https://www.sans.org/security-resources/policies/
- https://www.microsoft.com/en-us/nonprofits/security-privacy-compliance
- https://www.communityit.com/wp-content/uploads/2019/04/Community-IT-Cybersecurity-Playbook-2019.pdf
- https://www.communityit.com/wp-content/uploads/2019/03/NonprofitCybersecurityIncidentReport.pdf
- NIST Assessment Tool
  - Email meshleman@communityit.com for free access

THANK YOU!

CommunityIT Innovators®

where technology meets mission

www.communityit.com

cybersecurity@communityit.com