Cyber Risk

Speaker Introduction

Rick Spatafore

GISP, GCIH, HCISPP, CPHIMS, CHCIO

Sr. Manager, Advisory Services with Sentinel Technologies
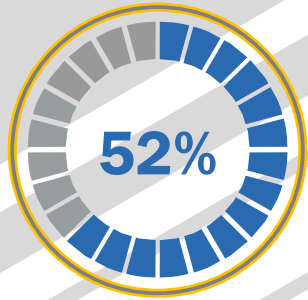
15+ years cybersecurity & compliance
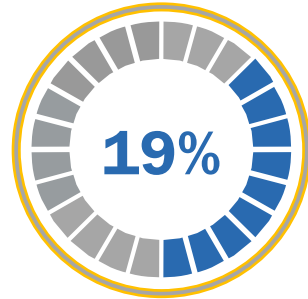
25+ years in technology
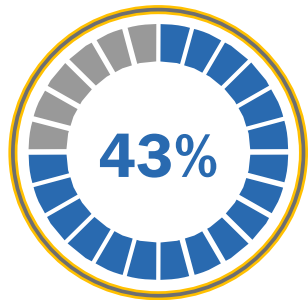
What is cyber risk?

Cybersecurity by the numbers

52%

Share of breaches caused by malicious attacks, at **an average cost of 8.64 million**

19%

of malware entered via email attachments. 73% of breaches were financially motivated & **27% were discovered by 3rd parties**

43%

of breaches by outside actors **25% involved inside actors**

Stolen or compromised credentials were the most expensive cause of malicious data breaches.

Breakdown of malicious data breach root causes by threat vector

Percentage of breaches caused by malicious attack

Social engineering 3%
Other 1%
Business email compromise 5%
Other misconfiguration or system error 6%
Malicious insider 7%
Physical security compromise 10%
Phishing 14%
Vulnerability in third-party software 16%
Cloud misconfiguration 19%
Compromised credentials 19%
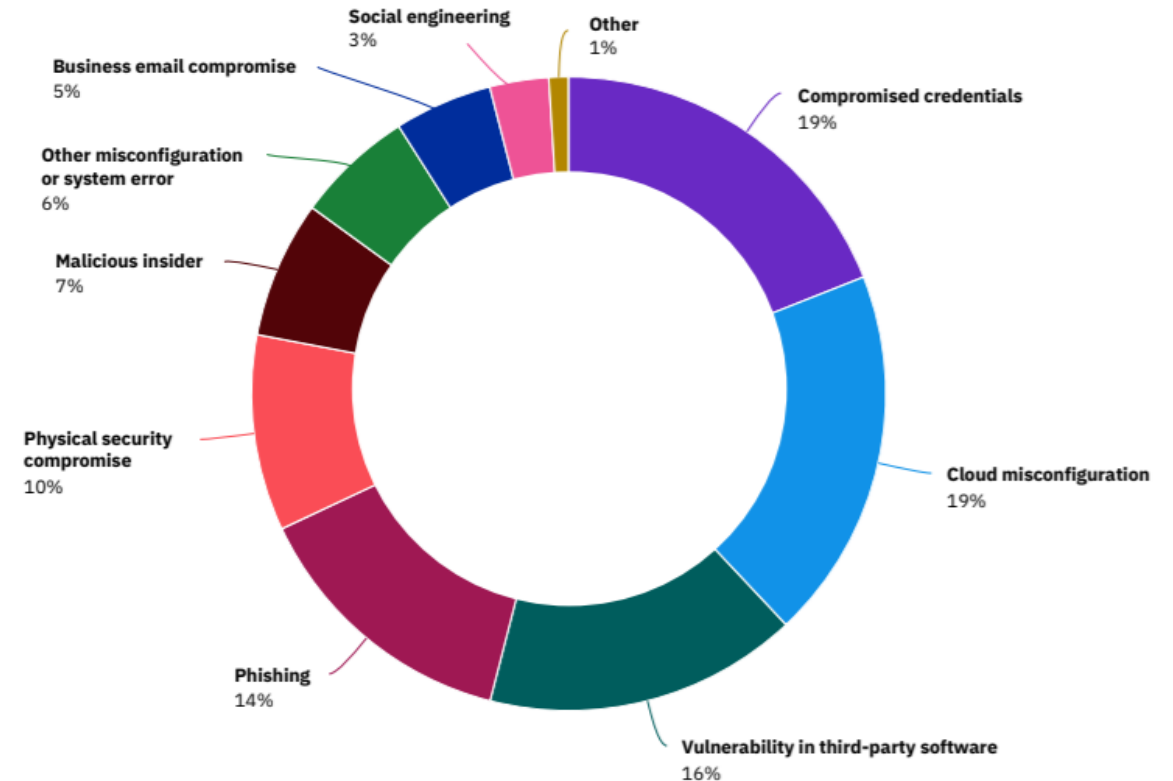
Education Risks

- Ransomware
- Phishing (Social Engineering)
- Malware
- Denial of service (DOS) attacks
- Unauthorized changes

Cost of a Data Breach

207 Days
The mean time to identify (MTTI) was 207 days.

73 Days
The mean time to contain (MTTC) was 73 days.

$8.64M
Average total cost of a breach in the United States

$-2M
Incident response (IR) preparedness was the highest cost saver for businesses

Sources: **2021 Verizon Data Breach Investigations Report**

Threats

Resources

Capabilities
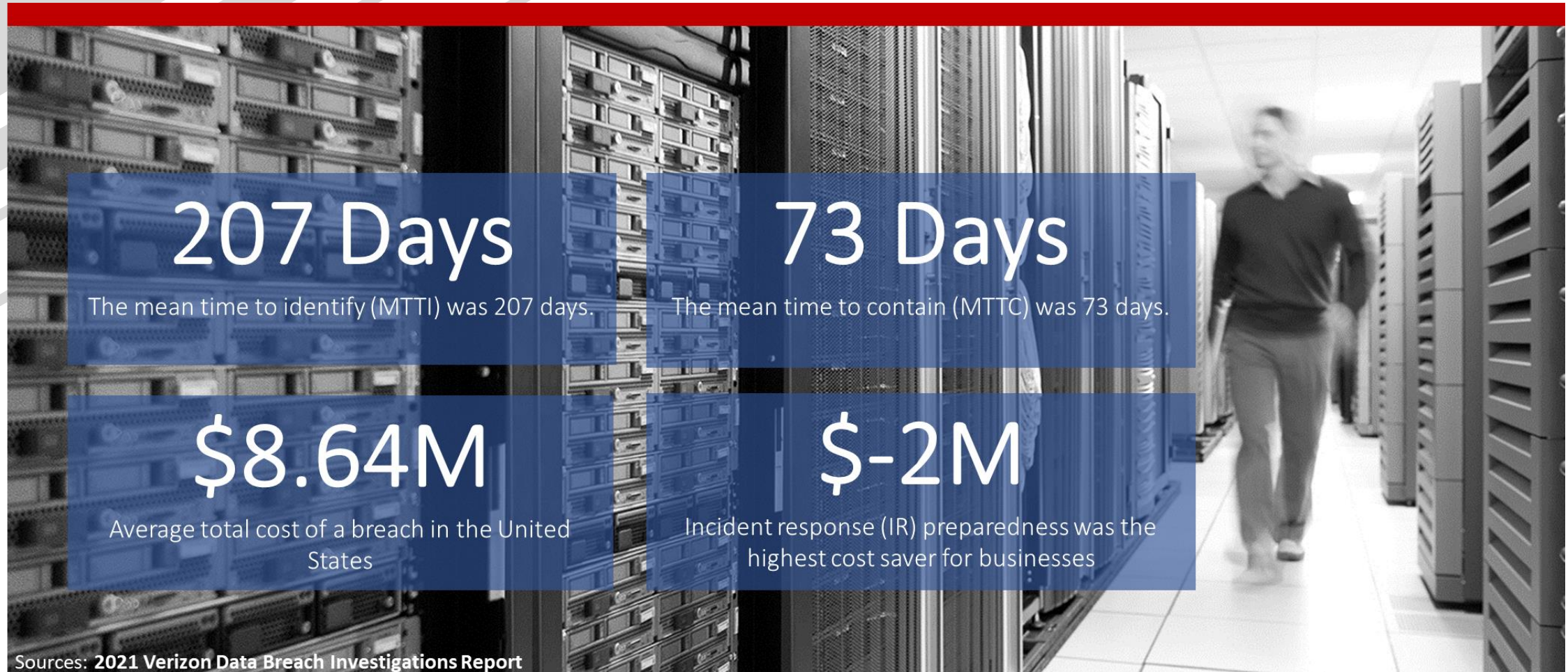
Security is not one size fits all

NIST Cyber Security Framework

IDENTIFY

Asset Management

Business Environment

Governance

Risk Assessment

Risk Management

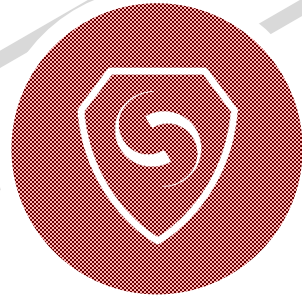Supply Chain Risk

Management

PROTECT

Identity Management

Access Control

Awareness & Training

Data Security

Process & Procedures

Maintenance

Protective Technology
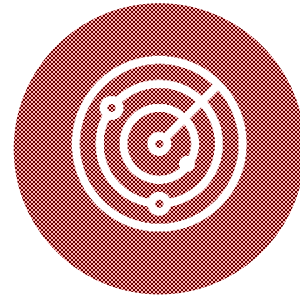
DETECT

Anomalies and Events

Security Continuous

Monitoring

Detection Process

RESPOND

Response Planning

Communications

Analysis

Mitigation

Improvements

RECOVER

Recovery Planning

Improvements

Communications

Cyber Kill Chain - Anatomy of an Attack

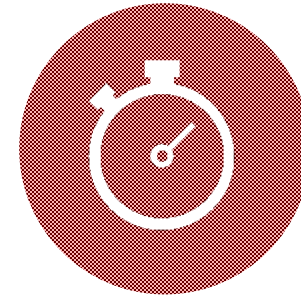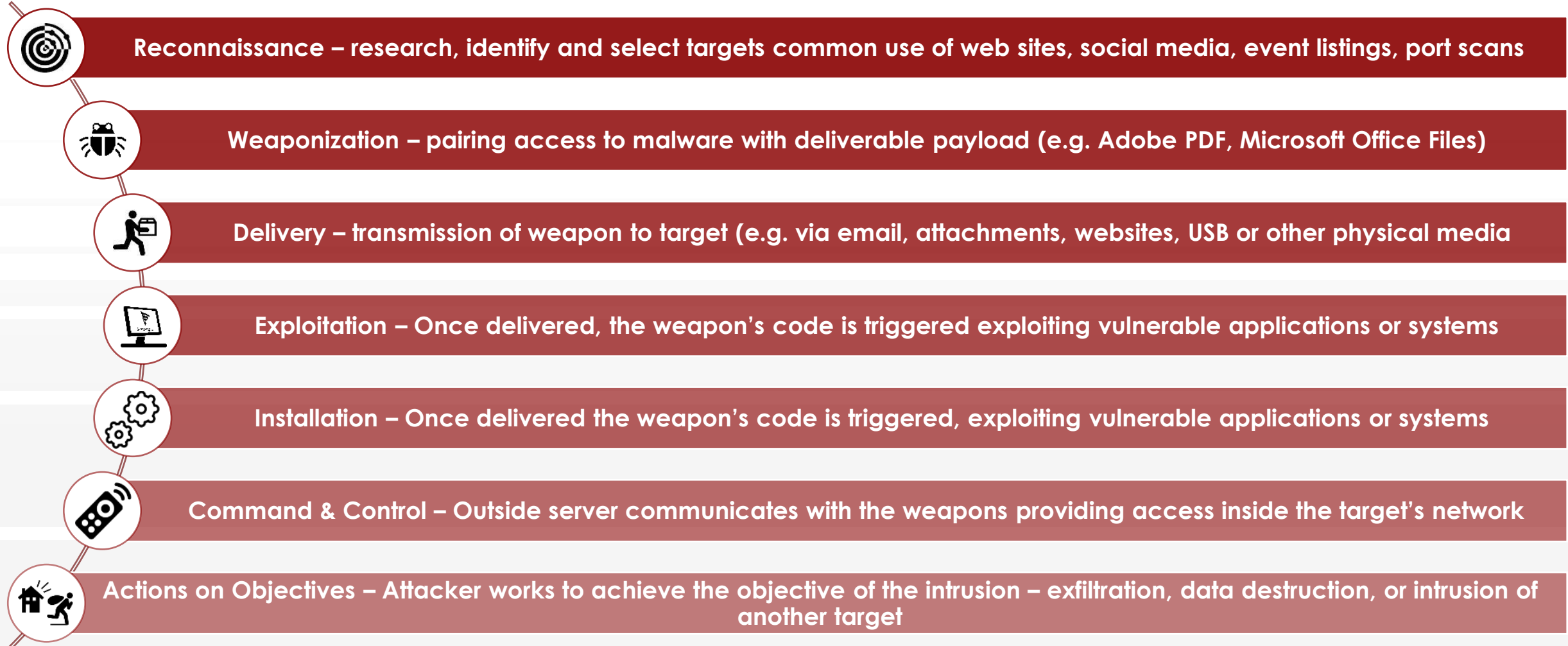**Reconnaissance** – research, identify and select targets common use of web sites, social media, event listings, port scans

Weaponization – pairing access to malware with deliverable payload (e.g. Adobe PDF, Microsoft Office Files)

Delivery – transmission of weapon to target (e.g. via email, attachments, websites, USB or other physical media

Exploitation – Once delivered, the weapon's code is triggered exploiting vulnerable applications or systems

Installation – Once delivered the weapon's code is triggered, exploiting vulnerable applications or systems

Command & Control – Outside server communicates with the weapons providing access inside the target's network

Actions on Objectives – Attacker works to achieve the objective of the intrusion – exfiltration, data destruction, or intrusion of another target

Passwords!!!

Password: x

It would take a computer about
7 HUNDRED PICOSECONDS
to crack your password

Password: Locu$t0%

It would take a computer about
9 HOURS
to crack your password

Passphrase: I like to vacation in Hawaii!

It would take a computer about
100 UNDECILLION YEARS
to crack your password

Where to start?
5 Recommendations

1. Multi-Factor Authentication - NIST CSF: PR.AC-7

2. User Education – NIST CSF: PR.AT
      All Users
      Third-party stakeholders
      Senior executives

3. Backups – NIST CSF: PR.IP-4
      Air-gapped and\or immutable

4. Vulnerability Scanning – NIST CSF: DE.CM-8

5. Incident Response Plan - NIST CSF: Respond
      NIST SP 800-61r2, SANS PICERL

Q&A

Contact Information:

Rick Spatafore
Sr. Manager, Advisory Services
Sentinel Technologies
Office: 630.786.8062
rspatafore@sentinel.com