

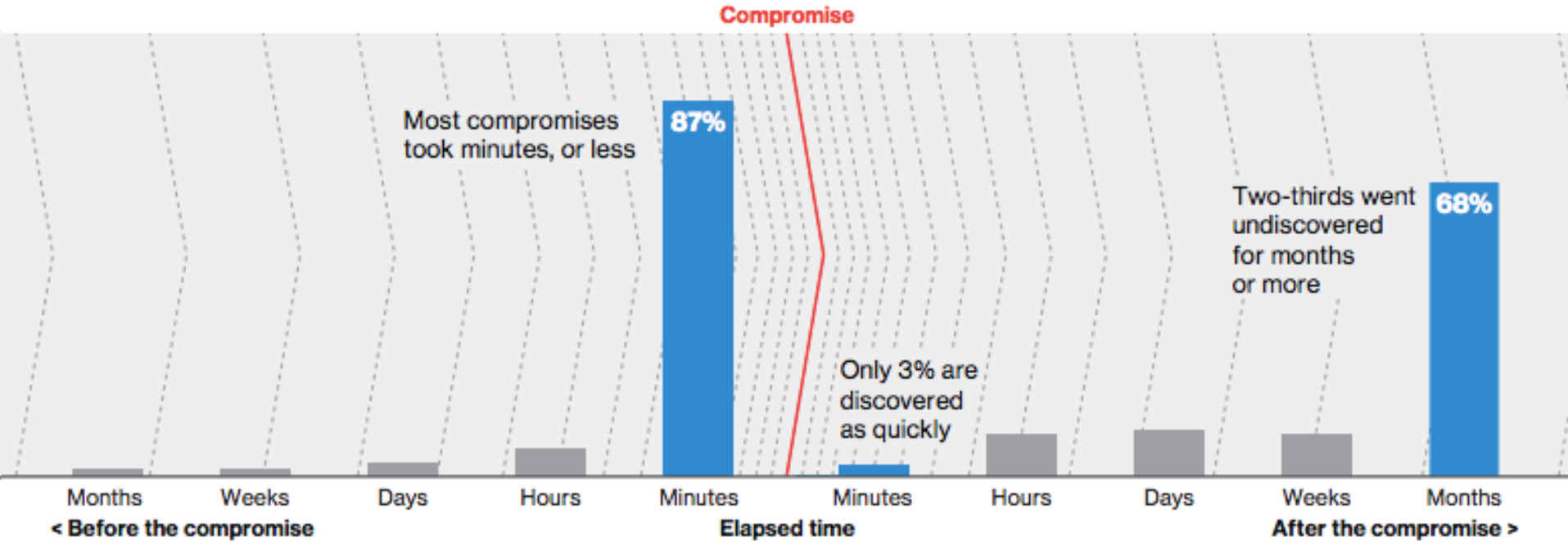
Cyber Threats and Trends for 2021

S. Allen Eaves, Jr. CISSP, CISM, CRISC, SSCP, CFE
Managing Director, Gladiator and Centurion

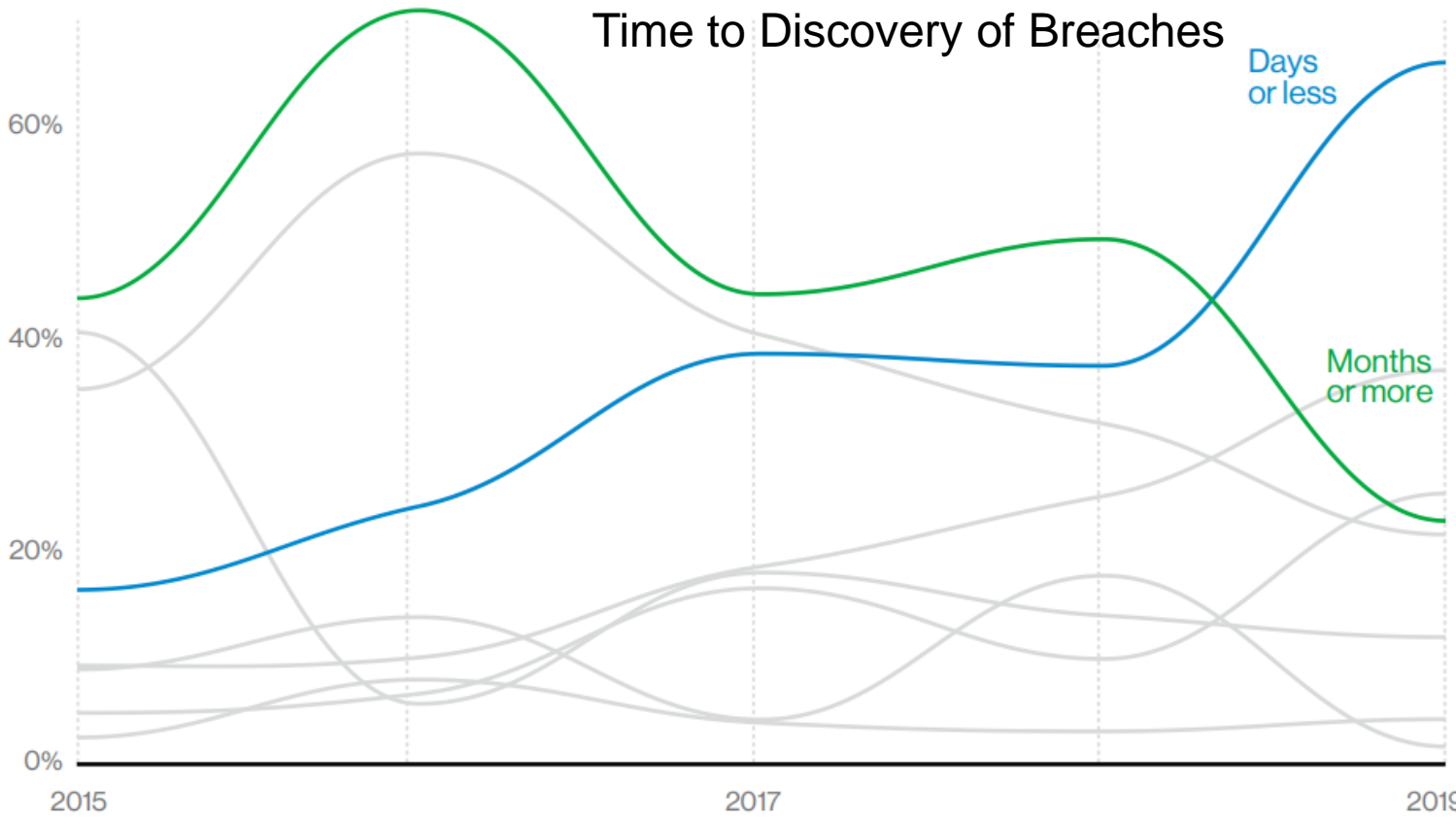
Predictions from 1/14/2020

- Increase in targeted attacks
 - Offensive/defensive machine learning/AI - 'Deepfake', Phishing and Vishing
- Attacker code appearing 'trusted' while privileges escalated
- Living off the land and evading detection
- Supply chain attacks
 - Remote-working setup vulnerabilities (IOT)
- Legitimate IT management tools used as malware
- State sponsored attacks - Iran
- Ransomware resurgence – double?
 - Targeting backups is routine

Verizon Data Breach Investigations Report - 2016

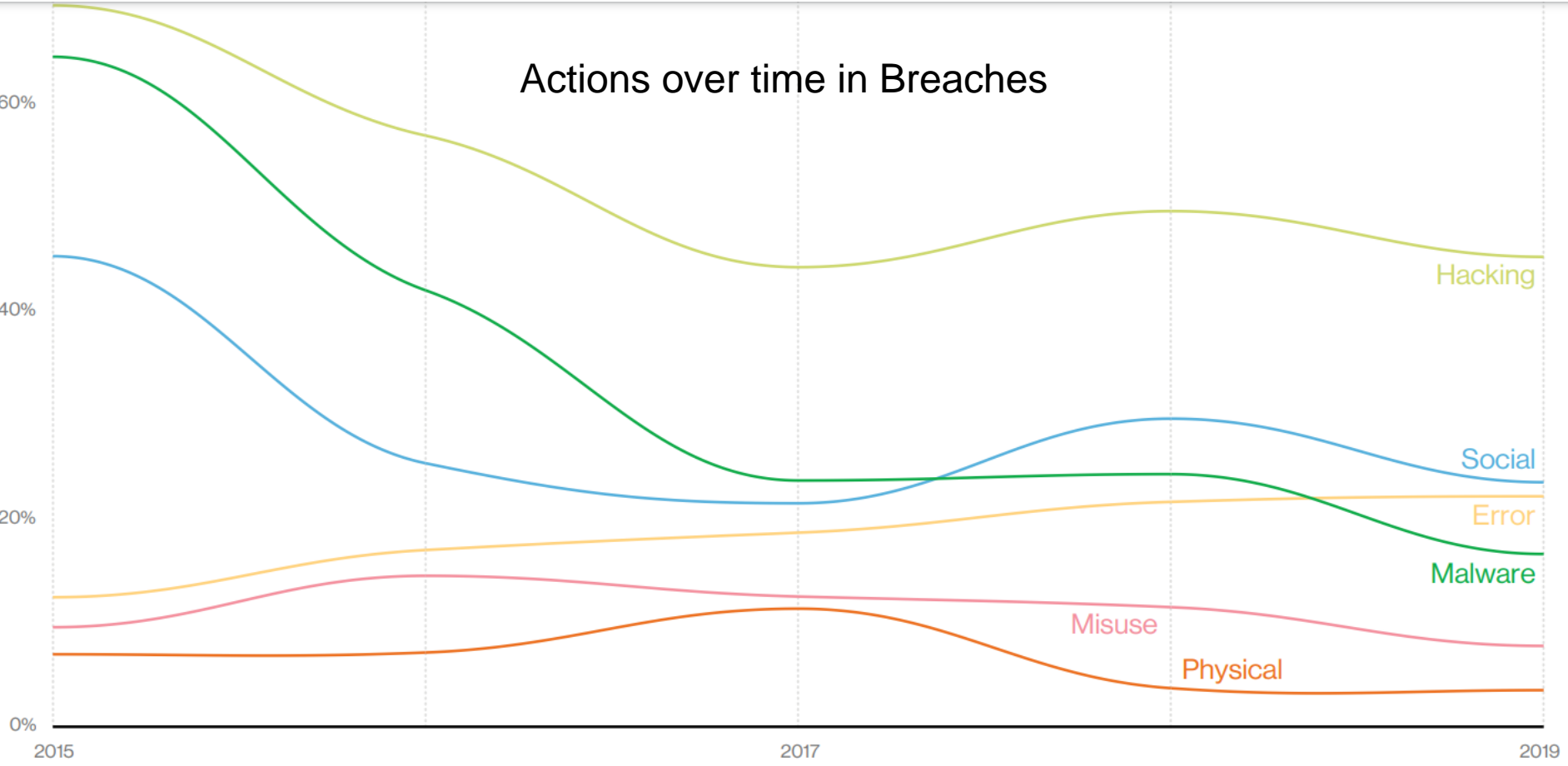


Verizon Data Breach Investigations Report - 2020



Verizon Data Breach Investigations Report - 2020

Actions over time in Breaches



- Fortinet's *Top Cybersecurity Statistics, Facts and Figures for 2021*
- FireEye and Mandiant's *A Global Reset: Cyber Security Predictions 2021*
- Splunk's *Data Security Predictions for 2021*
- AT&T Threat Traq Security Predictions
- RSA's *Cybersecurity Predictions for 2021*
- Verizon *Data Breach Investigations Report (2020)*
- F5's *2020 Phishing and Fraud Report (11/11/2020)*
- VMWare CarbonBlack's *A Look Ahead: 9 Cybersecurity Predictions for 2021*
- F5 Labs' *Cybersecurity Predictions for 2021 (1/6/2021)*
- BeyondTrust's *Top Cybersecurity Trends to Watch for 2021: The Hacking of Time, M/L Data Poisoning, Data Privacy Implodes, & More*
- Secure Futures by Kaspersky's *What does 2021 have in store for cybersecurity?*
- WatchGuard's *2021 Cybersecurity Predictions*
- Fortinet's *FortiGuard Lab's New Cybersecurity Threat Predictions for 2021*
- Symantec *2021 Cyber Security Predictions – Looking Toward the Future*

2021 Existing and Emerging Trends

- Exploitation of legacy endpoint's security weaknesses
 - Windows 7 and Server 2008
- Home Networks Targeted
- Continued surge of Phishing Attacks
 - ~72% of phishing sites using digital certificates and TLS
 - ~55% of phishing sites utilize the target brand names in URL
- Ransomware evolving – more automation
 - Increased extortion attacks

2021 Existing and Emerging Trends

- Legitimate IT management tools used as malware
- Supply Chain Attacks
- Increased regulatory pressure and stronger penalties
 - Federal breach notification requirements expanded beyond PII?
- Synthetic identity attacks – youthful targets
- Cybersecurity consolidation | Point solutions -> Cohesive
- Consolidated and more timely risk management
- Under-moderated social media hosting ripe for malware

So What?

- Encrypt critical and sensitive data.
Decrypt for Security Inspection.
- Use strong authentication, including MFA.



So What?

- Patch promptly after testing.
- Be vigilant. Implement systems for early breach detection.



So What?

- Make people and non-security staff an effective line of defense.
- Implement least-privilege. Keep data on a need-to-know basis.



The most reliable way to predict the future is to create it.

—Abraham Lincoln*

Cyber Threats and Trends for 2021

S. Allen Eaves, Jr. CISSP, CISM, CRISC, SSCP, CFE
Managing Director, Gladiator and Centurion