CIS Center for Internet Security®

The Value of Security Benchmarks and Controls

Curt Dukes

Executive VP & General Manager,

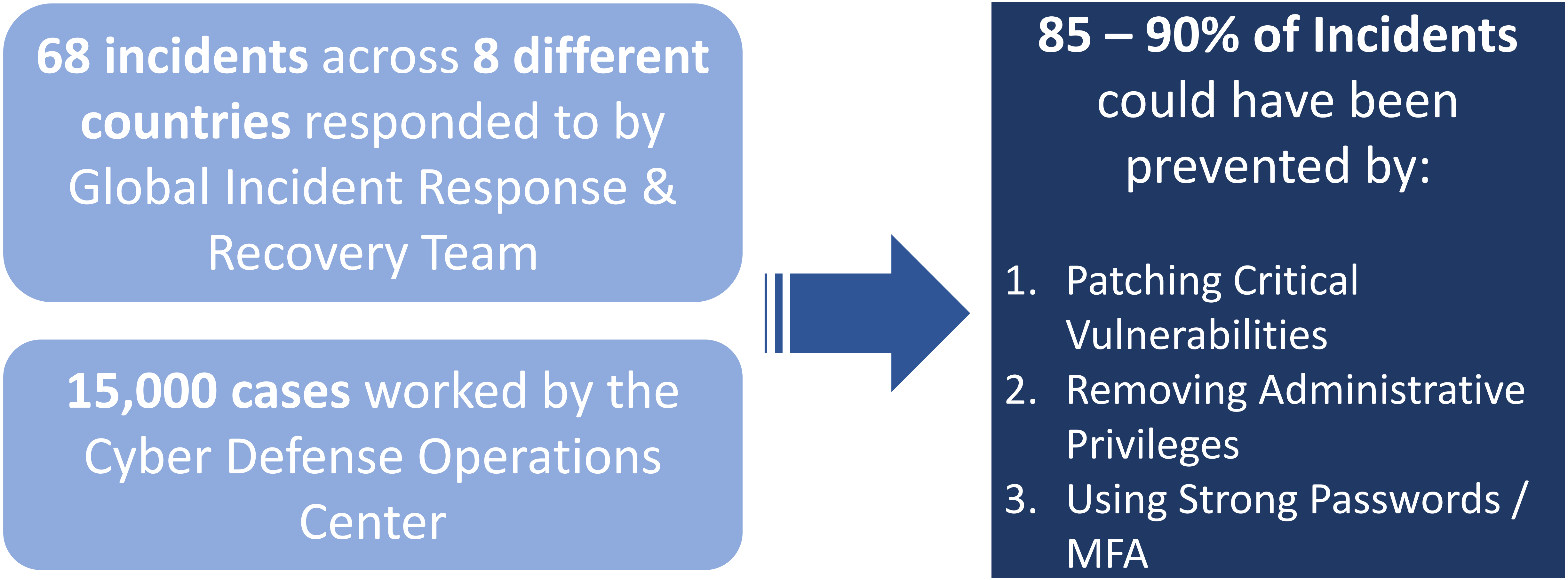
Security Best Practices & Automation Group

March 21, 2017

Some Unfortunate Facts

- The vast majority of compromises are based on known problems that have known solutions
- 85% of the incidents managed by the US-CERT come down to the same five basic defenses
- Very few attackers use “stealth” techniques
- Very few defenders have automated workflow

Threat Landscape – Last 6 Months



68 incidents across **8 different countries** responded to by Global Incident Response & Recovery Team

15,000 cases worked by the Cyber Defense Operations Center

85 – 90% of Incidents could have been prevented by:

1. Patching Critical Vulnerabilities
2. Removing Administrative Privileges
3. Using Strong Passwords / MFA

*Courtesy MSFT Security Research Center

“The Fog of More”

anti-malware

DLP

governance

certification

continuous monitoring

penetration testing

threat feed

baseline configuration

assessment

best practice

standards

SDL

audit logs

SIEM

virtualization

risk management framework

sandbox

compliance

encryption

threat intelligence

security bulletins

user awareness training

incident response

two-factor authentication

browser isolation

security controls

maturity model

need-to-know

supply-chain security

whitelisting

Even Foggier: Frameworks and Standards

ENISA Security Framework for Government Clouds

DHS Cybersecurity Framework

NISP DoD 5220.22-M

Bank of England CBEST

CISQ Automated Source Code Measures

NIST 800-53

COBIT

NATO CCD Cybersecurity Framework

NERC CIP

NIST CSF

ISO 27001/27002

PCI DSS

Healthcare Common Security Framework

ISF Standard of Good Practice

The Defender’s Dilemma

1. What’s the right thing to do, and how much do I need to do?

2. How do I actually do it?

3. How can I demonstrate to others that I have done the right thing?

The CIS Critical Security Controls

1) Inventory of Authorized and Unauthorized Devices

2) Inventory of Authorized and Unauthorized Software

3) Secure Configurations for Hardware and Software

4) Continuous Vulnerability Assessment and Remediation

5) Controlled Use of Administrative Privileges

6) Maintenance, Monitoring and Analysis of Audit Logs

7) Email and Web Browser Protections

8) Malware Defenses

9) Limitation and Control of Network Ports

10) Data Recovery Capability

11) Secure Configurations for Network Devices

12) Boundary Defense

13) Data Protection

14) Controlled Access Based on the Need to Know

15) Wireless Access Control

16) Account Monitoring and Control

17) Security Skills Assessment and Appropriate Training to Fill Gaps

18) Application Software Security

19) Incident Response and Management

20) Penetration Tests and Red Team Exercises

Focus on the first 6 Controls

- Know what you are protecting
  - ✓ CIS Control #1: Inventory of Authorized and Unauthorized Devices
  - ✓ CIS Control #2: Inventory of Authorized and Unauthorized Software
- Define Secure Configuration Baseline
  - ✓ CIS Control #3: Secure Configurations for Hardware and Software
- Continuously Monitor Vulnerability of Resources
  - ✓ CIS Control #4: Continuous Vulnerability Assessment and Remediation
- Limit and Monitor Administrative Privileges
  - ✓ CIS Control #5: Controlled Use of Administrative Privileges
- Continuous Monitoring/Situational Awareness
  - ✓ CIS Control #6: Maintenance, Monitoring, and Analysis of Audit Logs

- Website: www.cisecurity.org
- Email: Controlsinfo@cisecurity.org
- Twitter: @CISecurity
- Facebook: Center for Internet Security
- LinkedIn Groups:
  - Center for Internet Security
  - 20 Critical Security Controls