Taking Best Practices to the Next Level

Ken Muir

UZADO
Get Uzed to IT

KEN MUIR

Active in Information Security for over 24 years (started in IT in 1993)

Involved in building several successful cyber security startups

Experienced as a:

- ✓ Security Consultant
- ✓ Security Integrator
- ✓ Security Architect
- ✓ Senior Analyst
- ✓ Security Threat Hunter
- ✓ Managed Security Service
- ✓ Speaker
- ✓ Security Trainer
- ✓ Forensic Analyst
- ✓ Security Director

AGENDA

- Cybersecurity Threats – Now and Future
- Case Study In Good Security Practices
- Ransomware
- An Introduction to IOT (Internet of Things)
- Summary, Call to Action

INDUSTRY STATISTICS

Get Uzed to IT

$400 BILLION

Estimated global cost of cyber attacks annually

$1 BILLION

Estimated amount that was paid out in ransomware attacks in 2016

+60%

Of small businesses are out of business 6 months after a cyber breach

400,000

Machines that were infected by WannaCry in 2017

ESSENTIALS

Get Uzed to IT

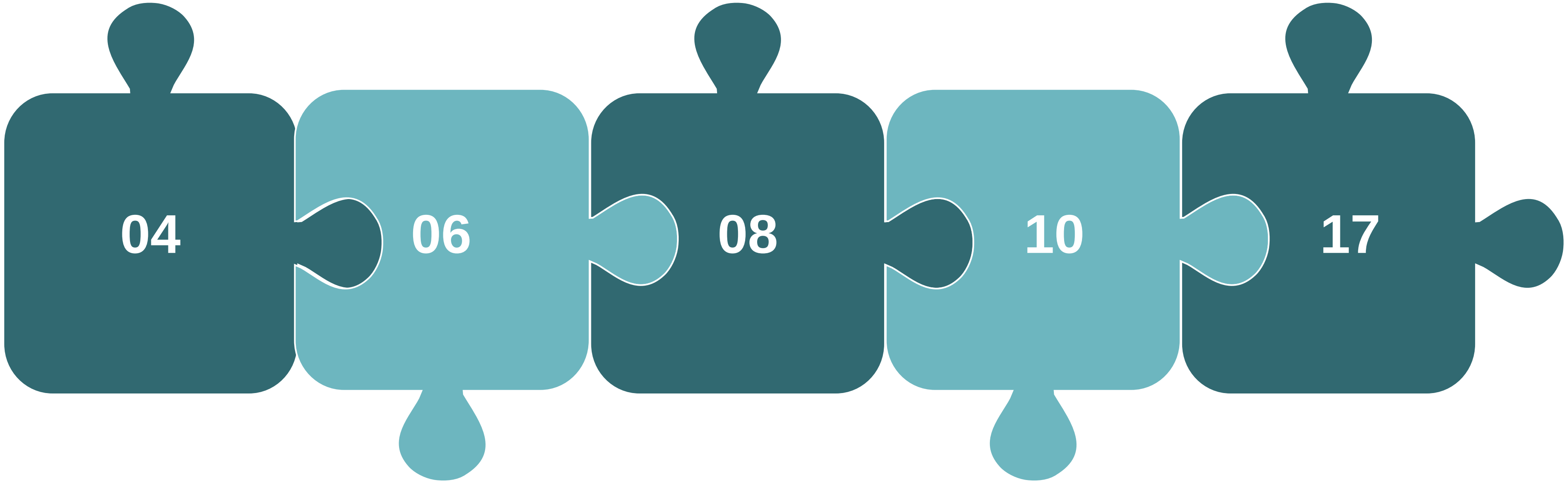
01 PATCH MANAGEMENT

02 NETWORK SCANS

03 SECURITY TRAINING

04 BACKUP & RECOVERY

CIS CSC CONTROLS



04 Continuous Vulnerability Assessment and Remediation

06 Maintenance, Monitoring, and Analysis of Audit Logs

08 Malware Defenses

10 Data Recovery Capability

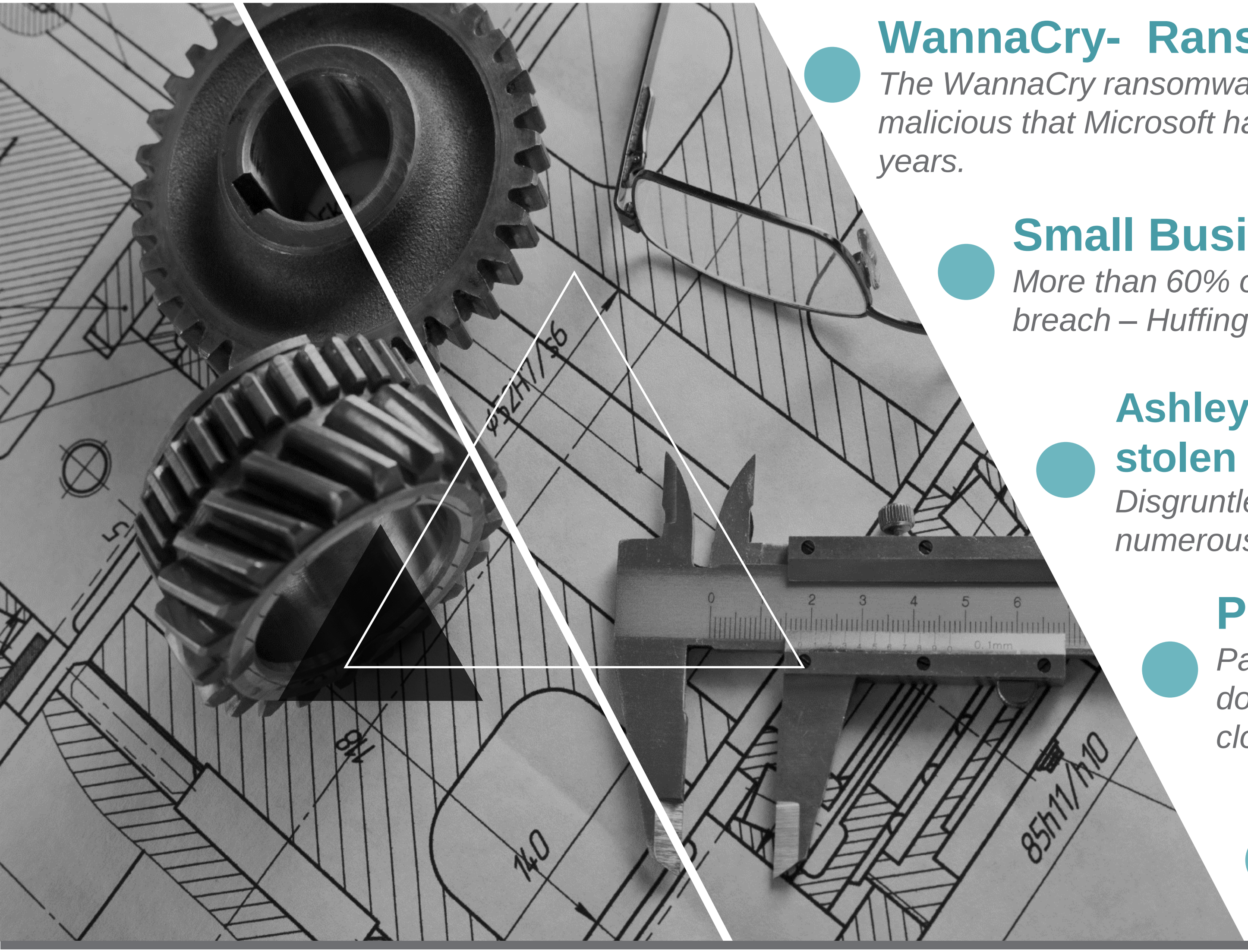
17 Security Skills Assessment and Appropriate Training to Fill Gaps

WHAT YOU'RE VULNERABLE TO

- ⚠ Phishing Attacks
- ⚠ Whaling Attacks
- ⚠ Malware
- ⚠ Ransomware
- ⚠ Other Forms Of Social Engineering
- ⚠ Viruses
- ⚠ Probing
- ⚠ Reconnaissance
- ⚠ System Compromise
- ⚠ Data Exfiltration
- ⚠ And So On…

MOMENTOUS BREACHES

Get Uzed to IT



- **WannaCry- Ransomware**
  The WannaCry ransomware became a global phenomena for May 2017, and has proven so malicious that Microsoft has issued patches for Windows versions dating back as far as 14 years.

- **Small Business Bankruptcies Due to Cyber Breach**
  More than 60% of small businesses are out of business 6 months after a cyber breach – Huffington post

- **Ashley Madison - Insider Job, 30+ million records stolen**
  Disgruntled employee stole client records. CEO stepped down, numerous instances of extortion, at least 2 reported suicides

- **Panama Papers - Phishing Exploit**
  Panamian Law Firm Mossack Fonseca compromised, 11 million documents stolen, Law Firm has been massively impacted, closing some location, losing lawyers and clients

- **Various Law Firms (primarily Canadian)**
  Mining company purchase, law firms breached, M&A data stolen, deal fell apart

(LACK OF) ORGANIZATIONAL VISIBILITY

Compliance Program

Compliance to industry standards (ex: SANS Top 20) is your guidebook to a more secure environment. Although, this has to be backed up by enforcement at a People, Process and Technology level

Full Scale Vulnerability Scanning

Vulnerability scanning and management is a vital part of checking real world risk to business systems and provides the visibility to verify remediation activity

Intrusion Detection/Prevention Capability

A key capability to analyze threats that increases the capability to thwart threats before they become a real issue

Employee Awareness Training

There are many free to low cost security training videos available online that can be used to train small to medium sized organizations

Defense-In-Depth Architecture

Standardizing on how and where critical business systems reside, and providing a layered approach to protection enables the reduction in risks associated with errors from individuals, as well as access enforcement.

CALLS TO ACTION

- ☑ Create/Improve a disciplined approach to threat management
- ☑ Don’t become complicit in propagating threats
- ☑ Get advice from a trusted advisor where you feel there are gaps

SUMMARY

Corporate Desire to Succeed

Successfully secure organizations, have made security a major part of their culture. Security teams are provided with the backing necessary to succeed. This is now, and has been for sometime, a business issue.

Policies, Process, People and Technical Enforcement

The combinations of these as a practice will significantly reduce overall risk

Educate Users

Users have traditionally been operating on the fringes of IT Security initiatives. Their lack of knowledge of good security principals is a recipe for disaster

Investing In Proper Visibility

Security teams need all available tools and capabilities to provide the views they need to reduce overall risks

UZADO
Get Uzed to IT

THANK YOU

Website:
www.Uzado.com

Phone Number:
(647) 847-4660

Email Address:
info@Uzado.com