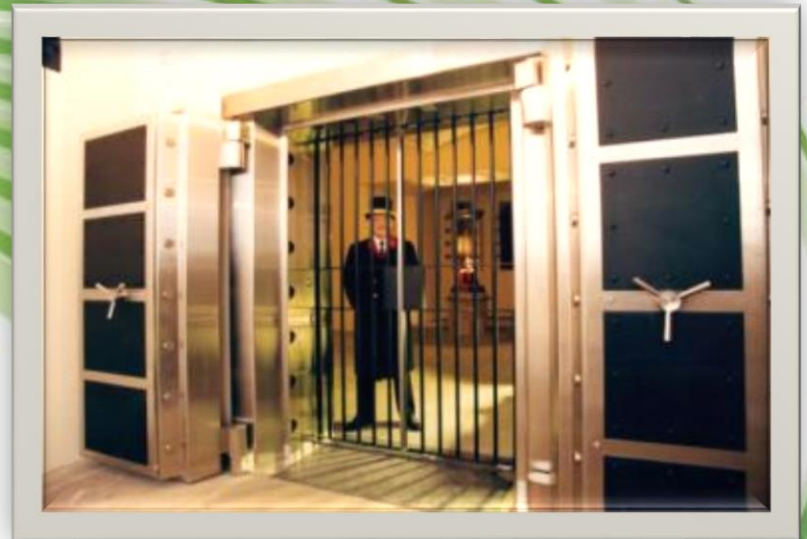


Are Your Systems Vulnerable to Hacker Attacks?

Achieving Success through Shared Experience

BC Ministry of Technology, Innovation and
Citizens' Services
Information Security Branch



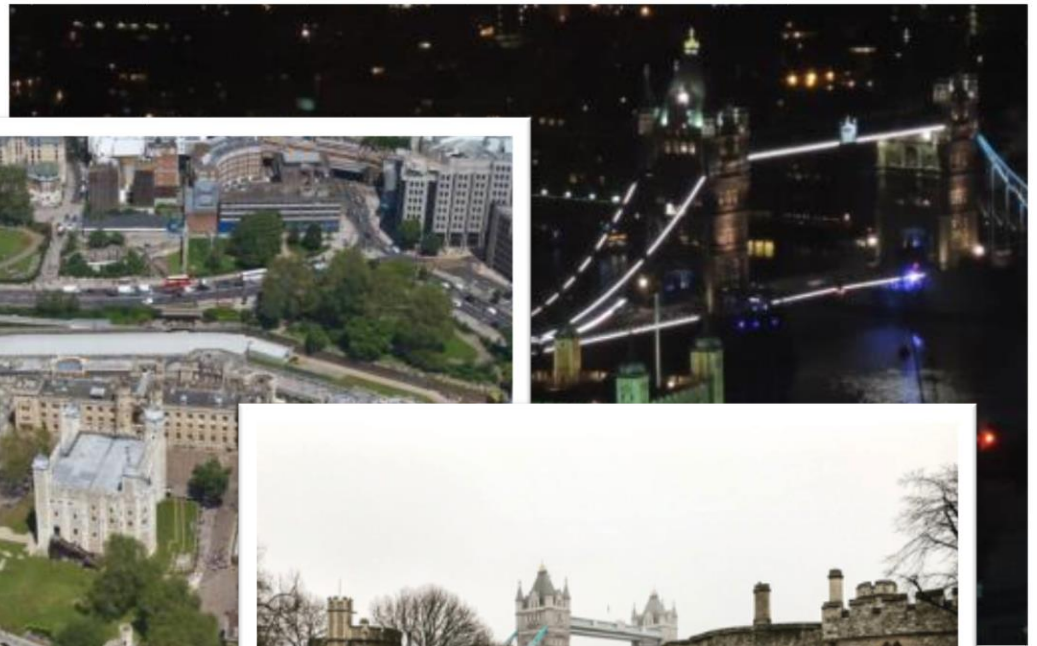
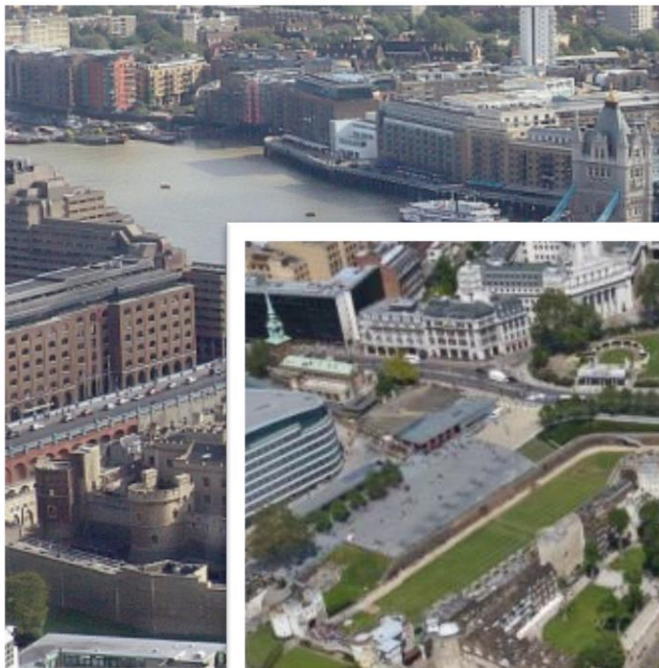
OCIO
Office of the Chief Information Officer

Agenda

- The Red Team / Blue Team Challenge
- Introductions
- Break
- Vulnerability Management Program
- Audits and Assessors
- Different Professional Perspectives of Vulnerability Management
- Questions

The Red Team / Blue Team Challenge

...Your role should you choose to
accept it



Here is your target: The Tower of London

Deep in the centre of the Tower lie the Crown Jewels.

Red Team Objective

- Break into the Tower of London and steal the Crown Jewels
- How will you breach the walls, get past the building security, access the fourth floor and steal the Jewels?
- What vulnerabilities do you see?
- What vulnerabilities can you exploit?



Blue Team Objective



- Keep the red team out of the Tower and keep the Crown Jewels safe
- What defenses do you have in place to keep the perimeter secure, the building secure and the Jewels out of the jewel thieves hands?

Introductions

- MI5
 - Gary Merrick
 - James Argue
 - Sherry Rumbolt
- Scotland Yard
 - Cornell Dover
- Jewel Thieves
 - Dom Kapac
 - Michael Cavallin

BC Government Vulnerability Management Program



BC Government Vulnerability Management Program

- What we do....
 - Multi-source information, analyse, assess risk, report risk and monitor for mitigation.
- What we don't do....
 - Accept Risk.



BC Government Vulnerability Management Program

June 2016

22,592

1

HIGH and CRITICAL vulnerabilities that are TRIVIAL to exploit

2

December 2016

292

1

...and we're not taking the foot off the gas

98.7%
reduction

Vulnerability Assessment

- Identify the vulnerability
- Identify the Impact
- Assess the risk
- Provide resources
- Recommend mitigation
- Provide timelines for resolution
- Continued assistance






























































Finding Vulnerabilities

- Scanning for targets
- Specific chosen targets



Vulnerabilities – Discovery

									
									
									
									
									
									...



No response



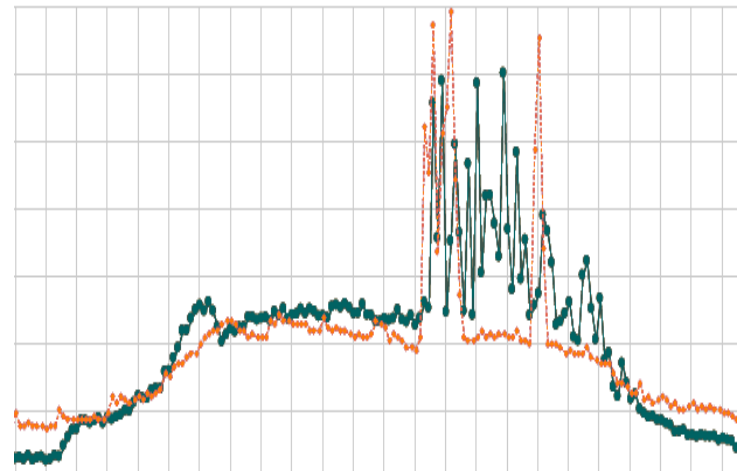
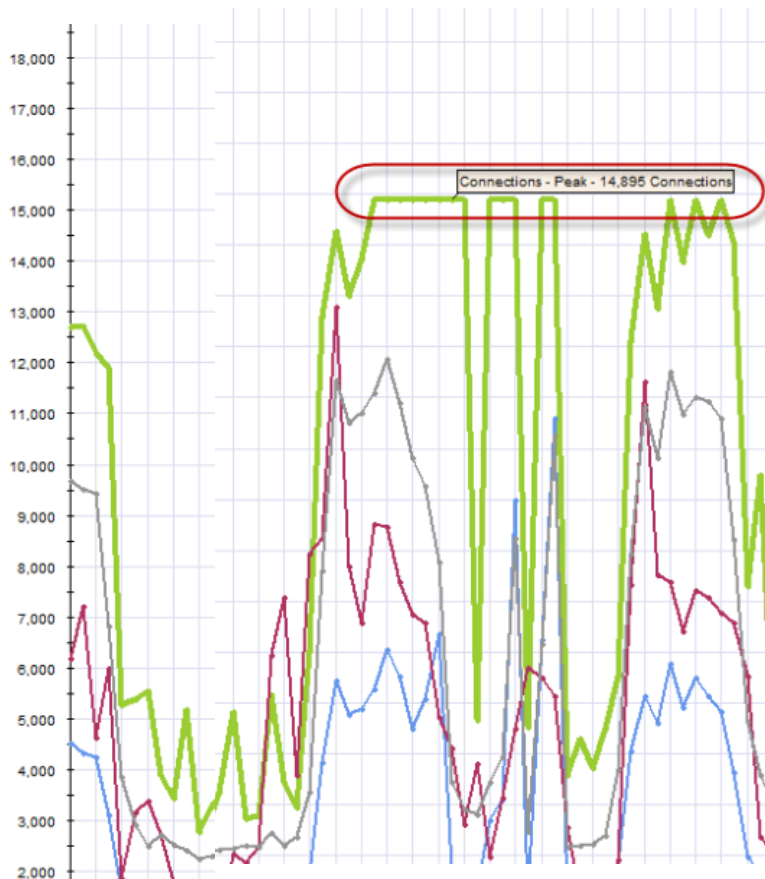
Service A



Service B

Vulnerability Scanning...Capacities!

- You never know what you will find in between the scanner and targets.



Specified Targets



- Client requested for specific services
- Deeper inspection under controlled circumstances
- Can be disruptive vulnerability testing, application testing, or both
 - Vulnerability tests = denial of service, writable directories, etc.
 - Application tests = “acting like a user”, SQL injection, login weaknesses, etc.

Specified Targets – What the client needs

- Credentialed or not (what credentials to use)?
- Time arranged for dedicated use of the targets
- Developer/business/other knowledge of the applications to interpret results
- Request for Change; other change management as required
- Business approval, business approval, business approval



Risk Assessment

- Likelihood

- Motivation
- Capability
- Opportunity



Planned Action

- Impact

- None
- Low
- Medium
- High
- Critical



Immediate Action

Remediation Next Steps – Manage the results

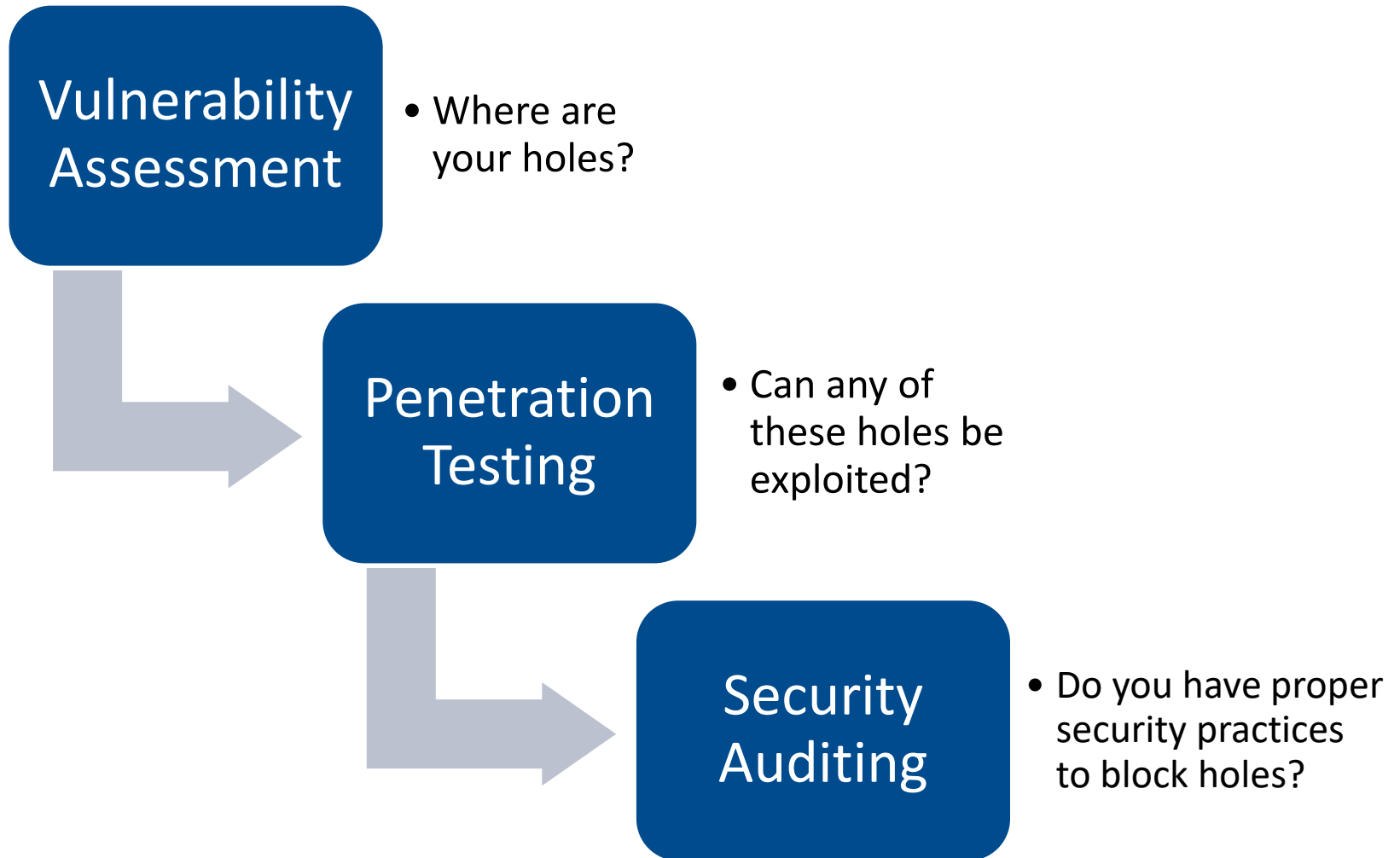
- Make recommendations for remediation
- Standard timelines to begin
- Compensating, deterrent, corrective, detective controls
- Track, log, follow-up
- Risk Register
- Escalation – as required



Audits and Assessors



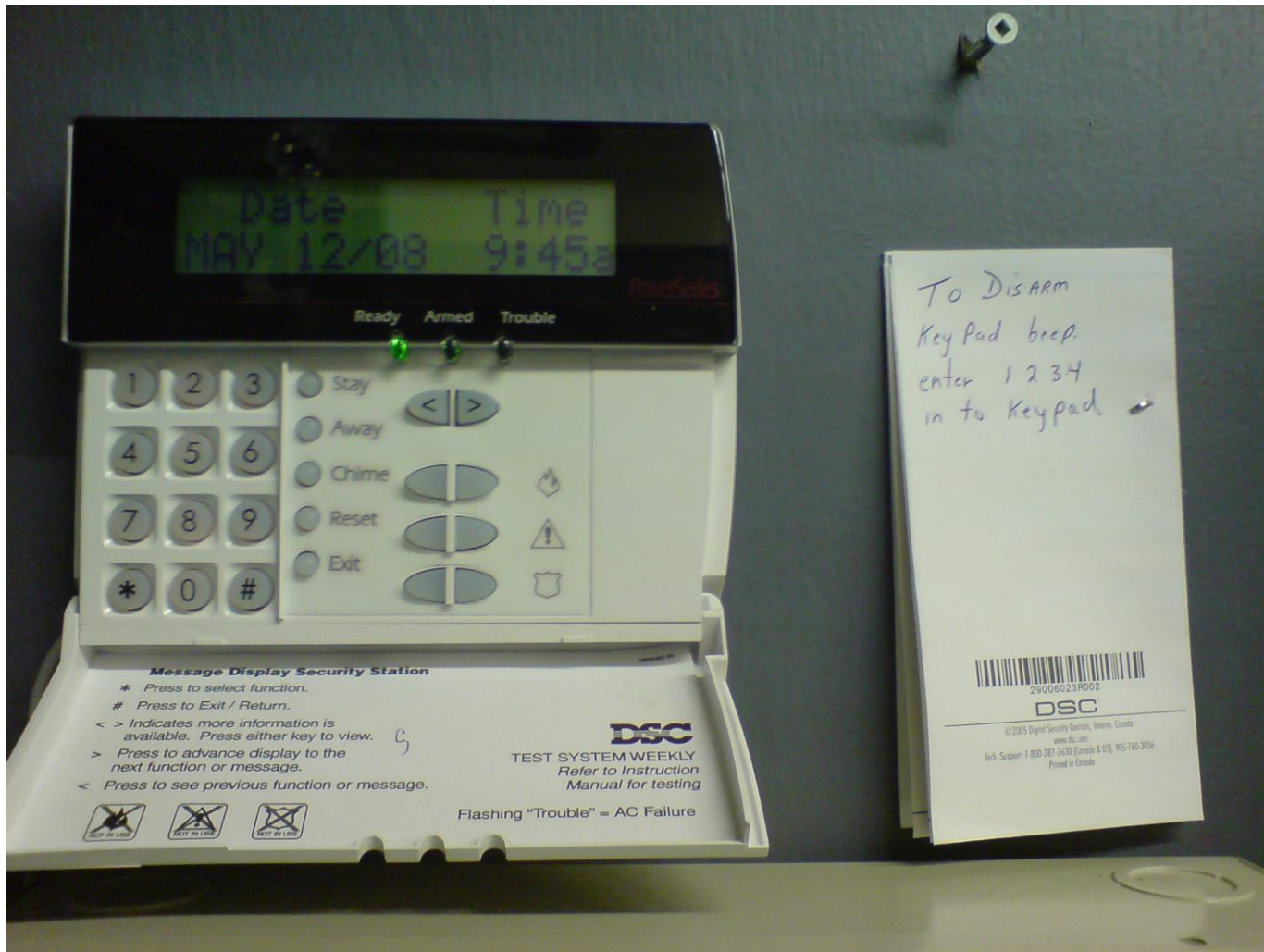
Vulnerability Management



Security Audit Basic Questions

- What do you have?
- Is it protected?
- How do you know?
- Can you prove it?

Audits Are Risk Based



Managing Risk Is An AART



Risk – Chance Of Loss

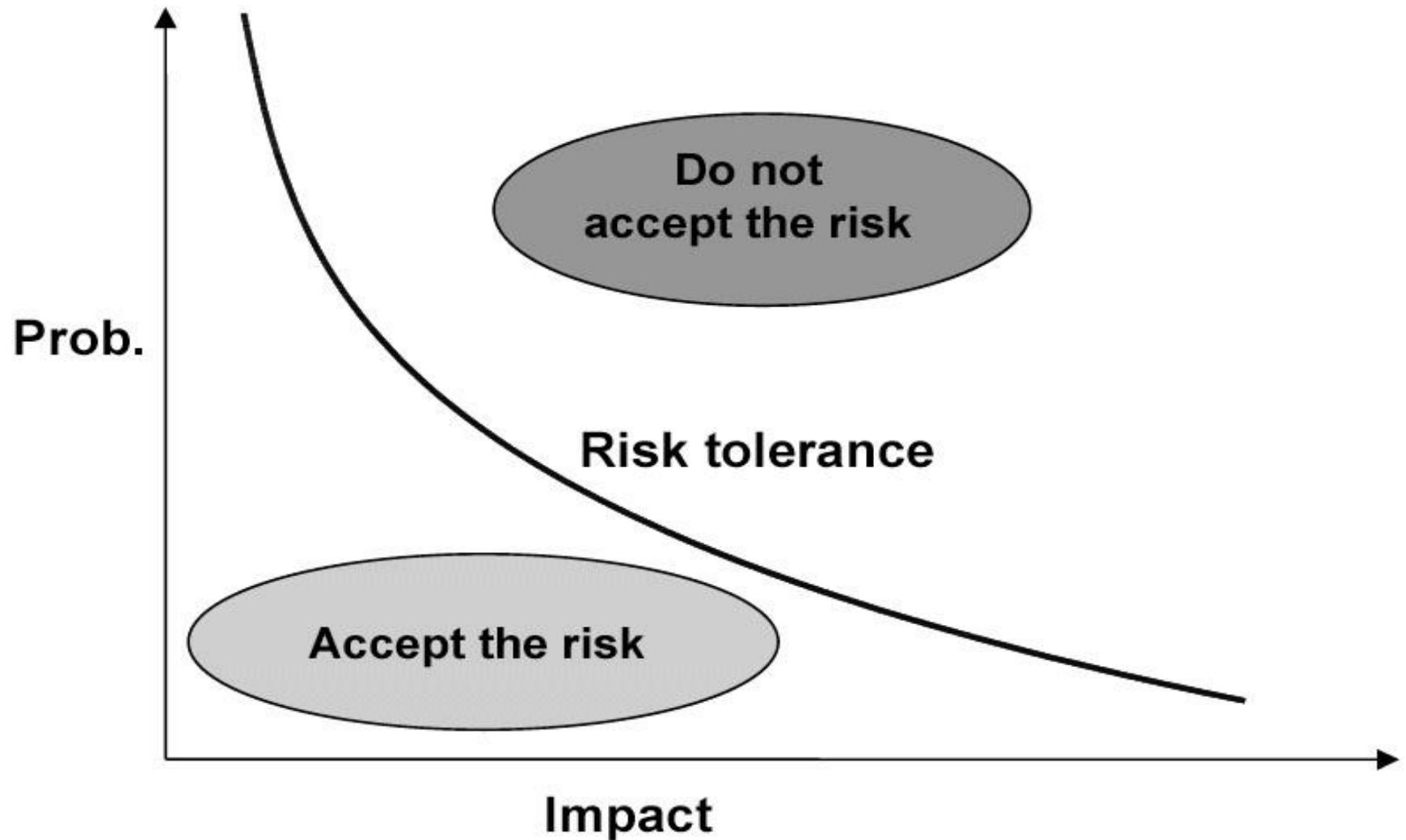




Risk Avoidance

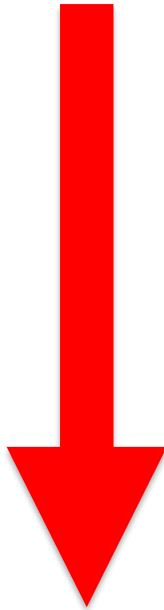


Risk Acceptance



Risk Reduction

Risk



Risk Transfer

Risk



REPUBLIC
FIRE INSURANCE CO.

TRUSTEES
ROBERT S. BONE, President.
CHARLES H. RUSSELL,
ROBERT S. MINTURN,
DANIEL B. PEARDON,
JOHN JACOB AFBOR, Jr.,
WILLIAM BUTLER DUNCAN,
HENRY G. BREWER,
BENJAMIN WITHERS,
JOHN A. C. GRAY,
PELEG HALL,
JOSEPH OAKES,
DENNING DUES,
HORTIMER W. HAMILTON,
JOHN STEWARD,
EDWARD C. CENTER,
FREDERICK G. PORTER.

TRUSTEES
WILLIAM H. RUSSELL,
GALATYAT E. LAMAR,
AUGUSTUS C. DOWNSING,
ARTHUR LEARY,
JAMES WARREN,
WILLIAM H. CART,
JOSEPH GAILLARD, Jr.,
JAMES M. WATERBURY,
GEORGE T. ADKE,
DANIEL DRAKE SMITH,
J. P. GIRAUD PORTER,
SAMUEL V. HOFFMAN,
JACOB ANTHONY, Jr.,
JOSEPH HOWLAND,
DUNCAN F. CURRY, Secretary.

THE PIONEER
MUTUAL FIRE INSURANCE CO.
COMBINING THE ECONOMY
OF THE MUTUAL PLAN,
WITH THE SECURITY OF A
CASH CAPITAL.

OFFICE
16 WALL ST. NEW YORK.

CASH CAPITAL \$ 150,000. SURPLUS OVER \$ 150,000.

BY THE CHARTER,
THE INSURED RECEIVE
80 PER CENT. OF THE
PROFITS, WITHOUT
INCURRING ANY PERSONAL
LIABILITY.

REPRODUCED BY
THE NEW YORK PUBLIC LIBRARY
AST LENOX TILDEN FOUNDATION
1901

Dec 31, 1861 446

Who Owns Risk?

Sure glad the hole isn't at our end



How to spend less time with the auditor



Different Professional Perspectives of Vulnerability Management



of devices connected
to the internet

6.4
billion

30%
Increase from 2015

5.5
million added
per day

30 billion by 2020

Internet of Things (IoT)

"starting this year" all of LG's home appliances will feature "advanced Wi-Fi connectivity." - LG marketing VP David VanderWaal, January 4th, 2017



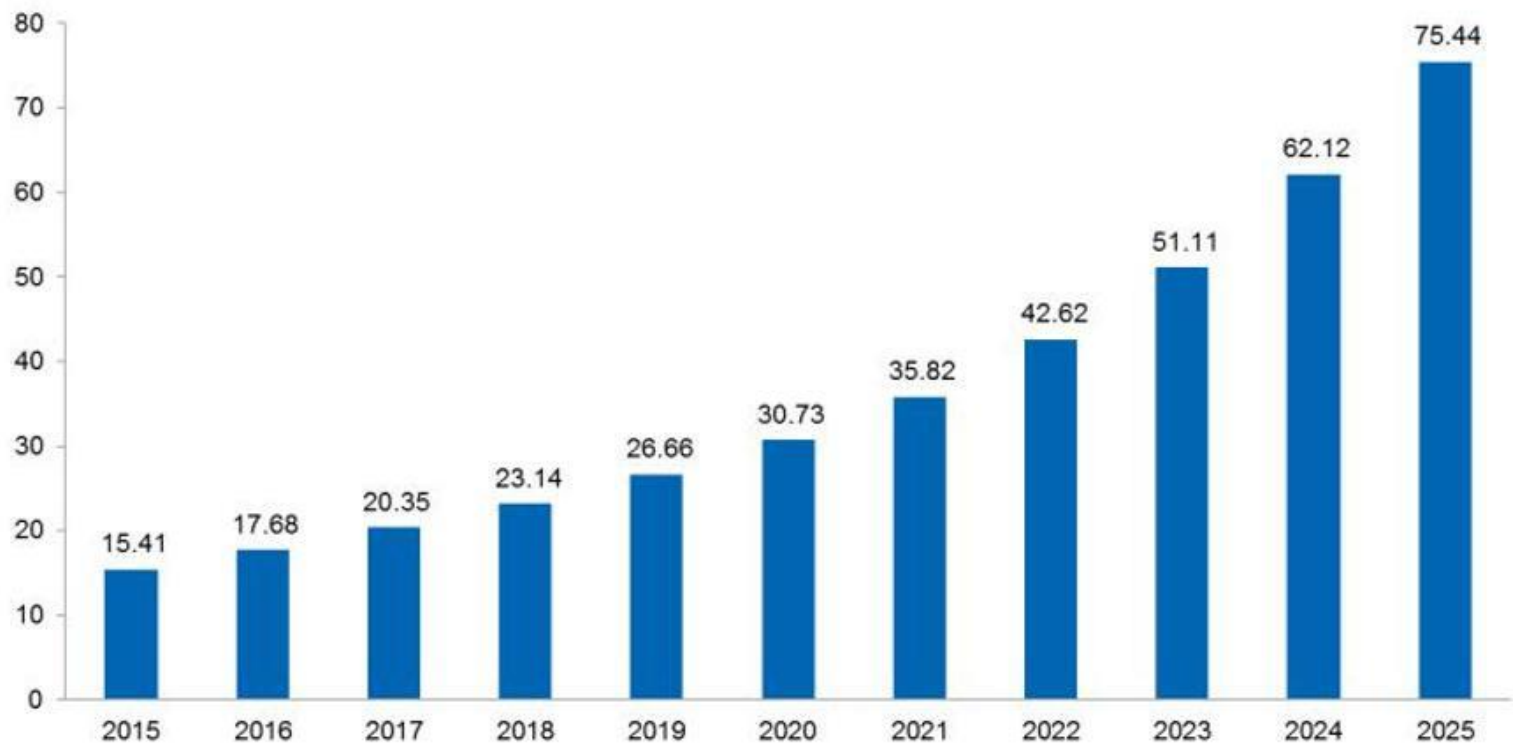
Internet of Things (IoT)



Internet of Things (IoT)

Figure 1. The IoT market will be massive

IoT installed base, global market, billions



Source: IHS

© 2016 IHS

Internet of Things (IoT)

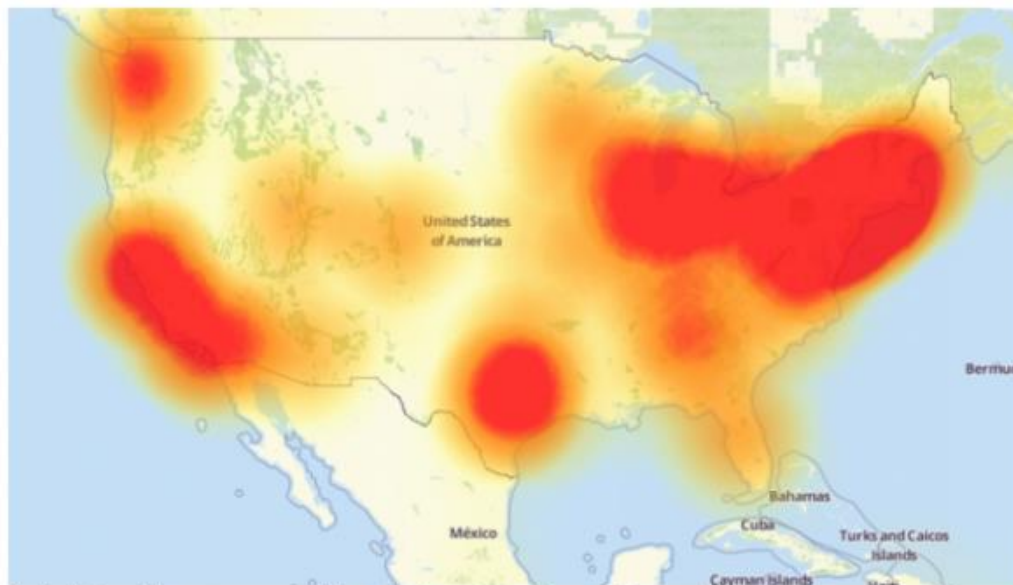


Internet of Things (IoT)

21 Hacked Cameras, DVRs Powered Today's OCT 16 Massive Internet Outage

A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked "Internet of Things" (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.



Earlier today cyber criminals began training their attack cannons on **Dyn**, an Internet infrastructure company that provides critical technology services to some of the Internet's top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.



A depiction of the outages caused by today's attacks on Dyn, an Internet infrastructure company. Source: Downtetector.com.

Internet of Things (IoT)

[Shodan](#) [Developers](#) [Book](#) [View All...](#)


 **SHODAN** 

[Explore](#) [Enterprise Access](#) [Contact Us](#)

New to Shodan? [Login](#)


[Exploits](#) [Maps](#)

TOP COUNTRIES



Germany	31,021
United States	27,769
China	23,017
Iran, Islamic Republic of	21,366
France	21,276


Total results: 280,369

106.37.236.181
181.236.37.106.static.bjtelecom.net
China Telecom Beijing
Added on 2017-01-17 23:15:38 GMT
 China, Beijing
[Details](#)

REGISTER sip:340200000020000000103402000000 SIP/2.0
Via: SIP/2.0/UDP 60.253.195.242:5060;rport;branch=z9hG4bk585916384
From: <sip:34020000001320000001@3402000000>;tag=453588133
To: <sip:34020000001320000001@3402000000>
Call-ID: 717551183
CSeq: 1 REGISTER
Contact: <sip:34020000001320000001@...

TOP SERVICES


HTTP	58,452
HTTP (81)	32,516
HTTP (8080)	20,220
HTTP (82)	17,411
Insteon Hub	10,429

62.90.212.13
62-90-212-13.barak.net.il
013 NetVision
Added on 2017-01-17 23:15:33 GMT
 Israel
[Details](#)

HTTP/1.1 200 OK
Server: Netwave IP **Camera**
Date: Tue, 17 Jan 2017 23:14:49 GMT
Content-Type: text/html
Content-Length: 2574
Cache-Control: private
Connection: close

TOP ORGANIZATIONS

Deutsche Telekom AG	19,616
ardebil telecommunic...	14,418
Orange	9,053
TOT	8,606
Sri Lanka Telecom	8,514

83.81.235.77
5351EB4D.cm-6-2d.dynamic.ziggo.nl
Ziggo
Added on 2017-01-17 23:15:32 GMT
 Netherlands, Alphen Aan Den Rijn
[Details](#)

HTTP/1.1 200 OK
Server: Netwave IP **Camera**
Date: Tue, 17 Jan 2017 23:15:19 GMT
Content-Type: text/html
Content-Length: 370
Cache-Control: private
Connection: close

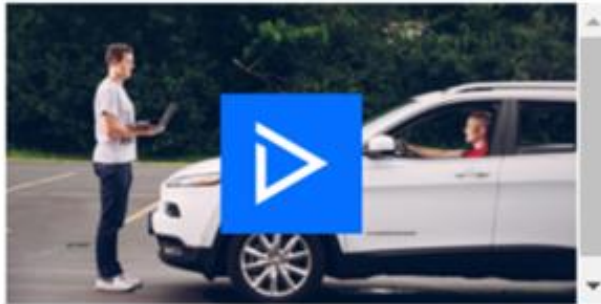
TOP OPERATING SYSTEMS

Internet of Things (IoT)



ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY— WITH ME IN IT



I WAS DRIVING 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

Though I hadn't touched the dashboard, the vents in the Jeep Cherokee started blasting cold air at the maximum setting, chilling the sweat on my back through the in-seat climate control system. Next the radio switched to the local hip hop station and began blaring Skee-lo at full volume. I spun the control knob left and hit the power button, to no avail. Then the windshield wipers turned on, and wiper fluid blurred the glass.

Question...

- **Would you permanently leave a stranger's computer connected to your home network?**



**Total Global Impact of CyberCrime [has risen to]
US \$3 Trillion, making it more profitable than the
global trade in marijuana, cocaine and heroin
combined.**

2013 Europol Serious & Organized Threat Assessment

What is a System Vulnerability

- A vulnerability is a flaw or bug in code of applications or systems some vulnerabilities are easier to exploit than others.
- A vulnerability can also be a person who is unaware of security practices (i.e. social engineering – the human element).



What Is An Exploit

- Code that is used to exploit a vulnerability within a system in order to gain access.
- When an exploit is successful, the attacker can drop payloads such as malware, including ransomware.
- Exploits can be used to gain unauthorized access but also to cause a denial-of-service condition.



Post Exploitation and Payloads



- A payload is any code or tool that allows interactions with the system after a successful attack
- Examples of Payloads include ransomware or a command prompt
- Tools to gain access to other systems within the network
- Tools to maintain access and extract data
- Malware (Trojans, ransomware etc.)

Parallels

- What are the parallels between the Towers' security posture and those of the Province? i.e. layered defences, security zones



Q&A

