Cyber Security – Bridging the Gap

THOUGHT(S) FOR THE DAY – BERKSHIRE BC FORUM

Alan Jenkins
Cyber Security & Convergence lead, ASIS UK Chapter & (by day) Associate Partner @ IBM Security UKI

07/10/2016
IBM is uniquely qualified to help secure a new era of computing

**INTELLIGENCE**
and Cognitive

Learnings from 35 billion security events managed per day

Real-time intelligence and cognition to help detect, assess, stop cyber threats

**INTEGRATION**
and Cloud

Integrated security services and technology solutions

Security for the cloud from the cloud

**EXPERTISE**
and Collaboration

Security best practices from tens of thousands of engagements

Platforms to share threat research and new apps
NCSC – National Cyber Security Centre

The National Cyber Security Centre https://www.ncsc.gov.uk/

Helping to make the UK the safest place to live and do business online

The National Cyber Security Centre, a part of GCHQ
Stood up as of 1st Oct 2016
External media references

https://www.youtube.com/watch?v=l0t3yDvQjww - Frank Abagnale/Watson interview
https://www.youtube.com/watch?v=hvc7A0x_fGs - IBM Films presents ‘Not a Breach’
https://youtu.be/nG36lKhy7ko - IBM Films presents ‘Hacked’
HOW DO WE OFTEN TALK TO THE BUSINESS?

But what does the business need/want to know?

What matters to your business (Execs & Non-Execs)?

*Reputation/stock price, revenue/cash-flow/results, EPS/shareholder value* ....
Cyber Security is not just for IT geeks!

How are you helping to protect your Enterprise, Clients & Suppliers against new and complex security challenges?

Some suggestions -
1. Talk to your IT/Information/Cyber Security colleagues …….
2. Ask them how you can help to:

   **OPTIMIZE YOUR SECURITY PROGRAM**
   Use experts to modernize security, reduce complexity, and lower costs

   **STOP ADVANCED THREATS**
   Use analytics and insights for smarter and more integrated defense

   **PROTECT CRITICAL ASSETS**
   Use context-aware controls to prevent unauthorized access and data loss

   **SAFEGUARD CLOUD AND MOBILE**
   Use IT transformation to build a new, stronger security posture
Cyber Security challenges are a complex puzzle

- **People**
  - Employees
  - Hackers
  - Outsourcers
  - Customers
  - Suppliers

- **Data**
  - Structured
    - Systems Applications
  - Unstructured
    - Web Applications
    - Web 2.0
    - Mobile Applications

- **Applications**
  - At rest
  - In motion

- **Infrastructure**
  - Datacenters
  - PCs
  - Laptops
  - Mobile
  - Cloud
  - Non-traditional
Today’s Cyber Security drivers

COMPLIANCE
HUMAN ERROR
SKILLS GAP
INNOVATION
ADVANCED ATTACKS

And not forgetting Cost-Benefit Analysis/Return-on-Investment/Value-at-Risk/Continuous Improvement!
Attacks break through conventional safeguards every day

<table>
<thead>
<tr>
<th>Year</th>
<th>Records</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>800+ Million</td>
<td>2014 1+ Billion</td>
</tr>
<tr>
<td>2015</td>
<td>Unprecedented</td>
<td></td>
</tr>
</tbody>
</table>

Average time to detect APTs: 256 days

Average cost of a U.S. data breach: $6.5M
Traditional IT Security practices are unsustainable

85 security tools from 45 vendors

1.5 MILLION unfilled cyber security positions by 2020

68 PERCENT of CEOs are reluctant to share incident information externally
Imagine if you could…

PROTECT against tomorrow’s risks, today
The next era of security

Moats, Castles

Intelligence, Integration

Cloud, Collaboration, Cognitive
## Establish security as an immune system

<table>
<thead>
<tr>
<th>Network visibility</th>
<th>Vulnerability assessment</th>
<th>Device management</th>
<th>Log, flow and data analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus</td>
<td></td>
<td>Incident and threat management</td>
<td>Fraud protection</td>
</tr>
<tr>
<td>Anomaly detection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transaction protection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privileged identity management</td>
<td></td>
<td></td>
<td>Access management</td>
</tr>
<tr>
<td>Criminal detection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sandboxing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtual patching</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Antivirus</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application scanning</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malware protection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application security management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fraud protection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transaction protection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident and threat management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data monitoring</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Content security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Endpoint patching and management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident response</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Enhance security through intelligence and integration

Global Threat Intelligence

Incident and threat management
Firewalls
Sandboxing
Virtual patching
Network visibility

Application scanning
Application security management

Data monitoring
Data access control

Consulting Services | Managed Security Services

Endpoint
Antivirus
Endpoint patching and management
Malware protection

Network
Transaction protection
Device management
Content security

Mobile
Fraud protection
Criminal detection

Advanced Fraud

Security Intelligence
Log, flow and data analysis
Anomaly detection
Vulnerability assessment

Applications
Incident response

Identity and Access
Privileged identity management
Entitlements and roles
Access management
Identity management

Identity and Access

Cloud
Intelligence

Advanced analytics for threat prevention, detection, and response

EXTENSIVE DATA SOURCES

IDENTIFICATION
• Data collection, storage, and analysis
• Real-time correlation and threat intelligence
• Automatic asset, service and user discovery and profiling
• Activity baselining and anomaly detection

REMEDIATION
• Incident forensics
• Around-the-clock management, monitoring and protection
• Incident response

Security Incident & Event Management, Sense Analytics Engine, Incident Forensics, Managed Security Services
IBM Watson Security Advisor determines the specific campaign, discovers more infected endpoints, and sends results to the Cyber Incident Response team.
Cloud

Monitor and enforce cloud usage

How is your business enforcing cyber security controls across its' hybrid IT infrastructure?
Collaboration: Leverage global threat research and intelligence sharing

Cataloging…

$88K^+$ vulnerabilities

$25B^+$ web pages, data from

$100M^+$ endpoints
RECOMMENDATIONS

1. Sign-up to WEF Cyber Resilience Principles to demonstrate business commitment
2. Set measurable business objectives for Security to deliver/enable/support revenue generation
3. Develop & then invest in Security Capability Improvement Programme
   1. Start with ID&Access Mgmt and Threat Intelligence coupled with Security Incident Event Monitoring
   2. Recognise that this is a Continuous Improvement programme, not a one-off Investment
   3. Review Enterprise (IT) Architecture to reduce risk of lateral movement once breached
   4. Develop & Test Business Continuity plans to improve Response & Resilience
4. Communicate what you are doing to both External & Internal stakeholders, eg Clients, Regulator & staff
   1. Improved Staff awareness is a critical success factor & something that many businesses can improve  (Quick Win)
5. Consider how best to reduce risk in your business' supply chain
   1. Flow down contract clauses & penalties for non-compliance; require Cyber Essentials (Plus) certification
   2. What are your critical information assets? What business outputs are dependant on which IT services/assets?
   3. Consider Privacy (Data Protection) implications of changing EU regulations
“Doing the same thing repeatedly
And expecting different results is
Insanity!”

Albert Einstein

We have an opportunity to mitigate what is currently an increasing business risk at some cost by improving what we already do and doing some things differently.

Failure is not inevitable if we act now but, not to act - to continue in the usual way - risks irrelevance and being considered of no value add.
Alan Jenkins

M: +44(0)7725095
E: aj@cybersecuritypilotage.co.uk / AJenkin3@uk.ibm.com
T: @aj66inuk
IBM Security key offerings

**OPTIMIZE YOUR SECURITY PROGRAM**
- IBM Security Strategy and Planning Services
- IBM Security Intelligence and Operations Consulting
- IBM Managed and Professional Security Services

**STOP ADVANCED THREATS**
- IBM Managed Security Services
- IBM Threat Protection System
- IBM QRadar Security Intelligence Platform
- IBM Trusteer Web Fraud Protection

**PROTECT CRITICAL ASSETS**
- IBM Identity and Access Management Software and Services
- IBM Security Critical Data Protection Program
- IBM AppScan
- IBM BigFix (Endpoint Manager)

**SAFEGUARD CLOUD AND MOBILE**
- IBM Cloud Security Software and Services
- IBM MobileFirst Security Solutions (MaaS360, AppScan, Access Manager, Trusteer)