Metrics – The Story So Far...

Phil Cracknell
@pcracknell

But first, an IoT interlude
IoT devices pose new challenge for security professionals?

- Only as much as Cloud adoption for personal storage or BYO did 😊
- Perimeters are disappearing entirely or becoming distant and weaker
- IoT Devices are introduced without consistent controls
- A typical data storage environment may have several points of ingress and egress now thanks to IoT Devices
- IoT Devices may want to call home
- You no longer have the same level of control in these environments

So protect the contents NOT the container!
IoT related threats

- Unseen/unknown egress and ingress to the home/workplace
- Lack of standards around the security of IoT devices
- Greater opportunity for devices to be hijacked and used to attack (DDoS)
- Increasingly embedded and therefore privileged access in many critical devices such as:
  - Cars (Accidents/Extortion/Disruption)
  - Medical devices (Death/Blackmail)
  - Wearable devices (Corporate espionage)
You probably don’t think about Florists. Last year, 34 florists in the UK had their websites taken down by DDoS attacks – (Distributed denial of Service) All on Valentines Day!

Most of those sites were taken down by other florists.
And so to the feature presentation

Metrics – The Story So Far...
Why not us?

• The Information & Cyber Security industry needs an effective, independent, common collection of metrics or security KPIs to provide the measurement and operational performance of the many elements defending our environment.

• In terms of finance, we can talk a common language regardless of the size, nature and industry of a business; EBITDA, PE Value, Days to Close, Finance Headcount Ratio
  • CFOs can quote them to each other as if they were playing Top Trumps
  • More importantly, CEOs and COOs understand them!

• Even our friends in IT have common values to indicate uptime, performance and operations

**Question:** So why has this universal unit of measurement evaded information security industry for so long?
Reporting – Why do we do it?

- We are asked for it by someone for an unknown reason/We’ve always done it
- It is expected from security
- We need to show bad things really are happening
- It secures security (IT) budget
- To know we are safe (Perceive that we are safe)
- To demonstrate a CISOs effectiveness
- To prove the security controls are working
- To validate a security purchase
- Because leadership need information that they may need to act upon
Are we reporting the WHOLE thing?

**Unknown unknowns**

- Unknown servers = unknown patched state = unknown vulnerabilities
  = unknown impact/likelihood of any associated risk

- Applications processing personal data that you don’t manage/know about

- Personally-owned devices unmanaged

- Breaches yet to be discovered
Changing the conversation

• Security leadership have been on a journey this last few years
  • To promote their cause, and to promote themselves!
  • Many CISOs don’t really operate at C-Level
  • Conflicted by reporting into IT

• The “Head of” security role is **critical** to the survival of businesses
  • This role has had a chequered past with the board
    • Trying to elevate their role, presence and influence in the business
    • Being notorious for saying NO to new initiatives
    • Shrouding themselves in mystery in terms of the detail and **not** being transparent in their activities
CISO meets CFO – location – coffee machine

CFO – Hey, how are we doing in security?
CISO – We had 55,000 viruses last month!
CFO – Oh, how many the previous month?
CISO – 60,000
CFO – Ah, things getting better?
  Or are we detecting less?
CISO – ...
er
CFO – What about that Malware outbreak you told me about last time, how much is that costing us?
CISO - ...
er
Reporting can be unintentionally misleading

Source: xkcd
Reporting can be intentionally misleading

• The millennium bug took the emphasis off security and on to business continuity for some time

• Industry FUD (Fear, Uncertainty and Doubt) rode on the shirt-tails of the Y2K bug
  • Vendors filled the void with news of new threats
  • Reports of breaches were NOT publicised and so-called “Intelligence” indicated new threats that were emerging
  • The vendor community maintained that companies were covering up breaches and so they pushed to promote their solutions to mitigate these theoretical risks

Note: Companies bought massively on the strength of such concerns.

They also spent disproportionately against the value of the assets they were trying to protect.
Reporting to law enforcement frowned upon?

How many data records were stolen last year in the UK? 1.9bn

How many cyber breaches were reported to the National Crime Agency last year? 100

Source: WIRED
Breaches start to hit the press

- TK/TJ Maxx – 2007 – 94 million customer records
- AT&T – 2008 – 130,000 accounts
- Heartland – 2009 – 130 million records
- Sony PSN – 2010 – 77 million user accounts
- Dropbox – 2011 – 68 million accounts
- Yahoo - 2012 – 3 billion user accounts
- Adobe – 2013 – 36 million accounts
- Ebay - 2014 – 145 million user records
- Target – 2015 – 70 million customer records/40 million card details
- FriendFinder – 2016 – 412 million accounts
Revisit the problem

• Reporting accurately and consistently has never been more important

• Being able to compare results with other companies, others in your industry sector or local geography are becoming popular board room requests

• We need:
  • Actionable information not speculation
  • Relevant intelligence
  • Data on recent risks or near misses not theoretical ones with low impact
  • Tools to inform others and gain traction with security from our peers

• We don’t need:
  • Scare-tactics which are intended to solicit a reaction/money/activities
  • Meaningless operational IT or Security detail (i.e. 55,000 viruses detected last month)
  • Individuals own “filter” on reporting/grading risks/issues of concern
The real value of metrics as part of structured reporting

- Enables senior stakeholders to see the things they need to be concerned about or take action against.

- Also demonstrates the positive impact of extra staff, additional training, increased budget for our technology defences etc.

- Is INVALUABLE in onboarding or due diligence exercises as part of a Merger or Acquisition.
Challenges to implementation

• Let’s not re-invent the wheel
  – we have valuable data right now

• However, if it’s not broken, let’s fix it anyway
  – but is there more valuable data that we should also be reporting against?
# The Metrics family

## Exposure

<table>
<thead>
<tr>
<th>Control Objective</th>
<th>Metrics</th>
<th>Sub-Process</th>
<th>Control Activity/Description</th>
<th>Risk</th>
<th>Mitigation</th>
<th>Goal</th>
<th>Sub-Process</th>
<th>Control Activity/Description</th>
<th>Risk</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>3rd Party Management</td>
<td>Exposure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Agilitey

<table>
<thead>
<tr>
<th>Control Activity/Description</th>
<th>Risk</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>3rd Party Management</td>
<td>Exposure</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Culture

<table>
<thead>
<tr>
<th>Control Objective</th>
<th>Metrics</th>
<th>Sub-Process</th>
<th>Control Activity/Description</th>
<th>Risk</th>
<th>Mitigation</th>
<th>Goal</th>
<th>Sub-Process</th>
<th>Control Activity/Description</th>
<th>Risk</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3rd Party Management</td>
<td>Culture</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Incidents

<table>
<thead>
<tr>
<th>Control Objective</th>
<th>Metrics</th>
<th>Sub-Process</th>
<th>Control Activity/Description</th>
<th>Risk</th>
<th>Mitigation</th>
<th>Goal</th>
<th>Sub-Process</th>
<th>Control Activity/Description</th>
<th>Risk</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3rd Party Management</td>
<td>Incidents</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Access & Controls

<table>
<thead>
<tr>
<th>Control Objective</th>
<th>Metrics</th>
<th>Sub-Process</th>
<th>Control Activity/Description</th>
<th>Risk</th>
<th>Mitigation</th>
<th>Goal</th>
<th>Sub-Process</th>
<th>Control Activity/Description</th>
<th>Risk</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3rd Party Management</td>
<td>Access &amp; Controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Project “metrics”

• Businesses are waking up to the fact that they need metrics/risk indicators that our board, audit committees and non-exec directors understand, for they are the key to budget, extra staff, a corner office and a job for life

• It’s not uncommon to get that Monday morning swoop-by when the CEO has read something in the Sunday Times and wants to know;

  “Where are we with that one?”
  “Have we started preparing for GDPR (Insert next big thing here…)?”
  “What are other companies doing?”

• Metrics, as the project group of CISOs originally decided to call them, are the key to our future

• They are being defined by CISOs alone, they detail exactly how we demonstrate our effectiveness, pinpoint our responsibilities and highlight investment or lack of it
How it all began...

• Put 25 CISOs together in a room with Post-It notes pads, marker pens and a huge glass wall and magic starts to happen

• The group, with a combined 350 years of information security experience to write down what they considered to be their top five metrics.
  • Five things that they think were the most important measures of security effectiveness

• The results showed three or four general ‘headings’ or families into which the majority of post-it notes fell. This was our starting point.

• It’s not just about creating a framework for metrics. We chose to establish a second workstream to lobby, educate and inform audit committees, data privacy officers, non-exec directors and influencers on what exactly the metrics could tell them.
Metrics – top level – take 1

- Exposure
- Agility
- Culture
- Incidents
- 3rd Party Management
- Access & Controls
Metrics – top level – take 2

- Exposure
- Agility
- Culture
- Incidents
Exposure

- The **numbers of systems** which are vulnerable to an attack/exploit
- Represents unpatched, unprotected and unknown levels of security
- Can be detailed to show public-facing, DMZ, 3rd-party-facing and internal systems
- Shows critical application exposure
- Also can show application exposure through calling external libraries
Agility

• The **number of days** it takes to patch systems which are vulnerable to an attack/exploit (See exposure)

• Refers to unpatched, unprotected and unknown levels of security and how quickly your organisation can remediate them

• Can demonstrate change management inadequacies
Culture

- Staff awareness is a key metric in this group, the **number of new starters given awareness training** for example and in what timescale from them joining
- Staff turnover, leavers, movers joiners can be scrutinised
- Executive attitude and appetite for risk can be reflected here
- Risk management process and maturity
Incidents

- **Number of major security incidents**, minor incidents
- Internal incidents
- Near misses
- Breach disclosures
- Ico or pci non-compliances
How it could all fit together to feed a dashboard:

- **PRA Questionnaire**
- **Metrics**
- **Risk Categories & Assessment Values from Risk Team**
- **Dashboard**
  - Cyber & Information Security Dashboard
  - Updated every 5 minutes
    - Exposure
    - Agility
    - Culture
    - Regions (Global)
    - Status
    - SIP Issues
    - Mobile Device Assets
    - Vulnerabilities
    - Incidents
  - Risk Scorecard
  - Audit Actions
Or mapped to other existing reporting mechanisms
So we are looking for end-user CISOs/Security Managers to join us in this next exciting phase...

http://www.themetricsproject.co.uk