STORM Guidance

Strategic, Tactical & Operational Risk Management

Neil Hare-Brown

The Cyber Risk Pandemic

Assess | Plan | Respond

On the Menu

- Introduction
- Realising the Cyber Risk Need: Past & Future
- The Evolution of Cyber Risk
- Cyber Risk Assessment Options
- Cyber Risk Indicators: The Seven Deadly Sins
- Cyber Risk & Loss Quantification
- Future Predictions

STORM Cyber.Care: Assess|Plan|Respond

Full Service offering for Reinsurers, Insurers, Brokers and Clients

Cyber.Care|Assess: lightweight cyber risk assessments to enable clients to learn and improve their cyber security and to enable insurers and reinsurers to manage book risk

Cyber.Care|Plan: helping insured clients to create, learn (through training) and exercise/test their plans in dealing with different types of cyber incidents in the context of their business. Infosheet attached.

Cyber.Care|Respond: delivering a fully coordinated and Integrated Cyber Incident Response Team (I-CIRT).

ReSecure
Data Breach Response

Cyber|Decider: world-first cyber insurance policy comparison engine

Cyber|Decider

STORM Guidance
Assess | Plan | Respond

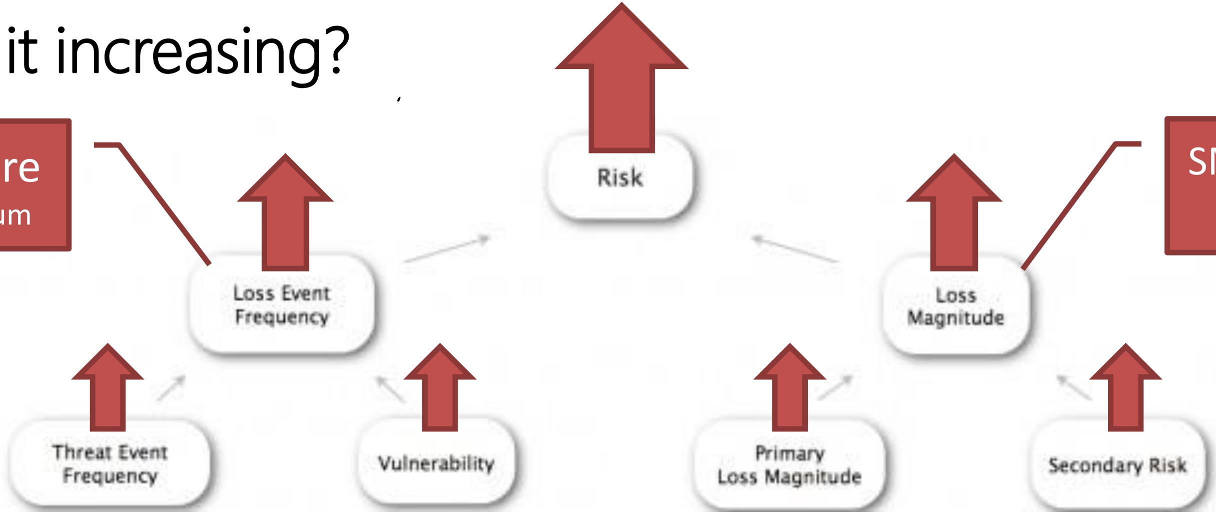
Realising the Cyber Risk Need: Past & Future

Working to Build the New Cyber Market

- Realisation that reliance on IT (and criminal use of it) resulted in a growth in incidents of theft/fraud and business interruption
- Businesses increasingly unlikely to easily absorb worst-case losses
- Real opportunity for cyber insurance to drive improvements which have eluded business and led to a poor state of cyber resilience
  - To achieve what government policy & regulation has failed to attain
- Insurer-Intermediary-Client relationship will need better communication
  - Requiring a continuous improvement cycle

What is Cyber Risk?

Why is it increasing?



x14 than fire
Avg. 2 per annum

SME £200,000*
LG £1.4m**

Internet Growth
Automated Tools
Jurisdictional Boundaries

IT complexity
Lack of Skills
Lack of Investment

High Reliance on IT
Online Transactions

Consumer/Business
Expectation
Legal Obligation

Typical Loss
* RAND (2016)
** PwC (2015)

The Evolution of Cyber Risk

Growth of Online Services = Increase in Cyber Risk

- Security was not an original design feature of the Internet or PC technology
- The drive for online business growth has overridden those calling for consideration of security needs – this trend continues (& worsens) with IoT.
- ‘Follow on/Wrapper’ security functions are complex and ineffective
- Governments & businesses have not invested sufficiently in skills required & IT budgets remain relatively low
- Many IT Security vendors have sold ‘snake oil’ security products
- Most programmers & website designers have little ability to ‘design for security’
- Jurisdictional complexity means ‘risk of prosecution’ to criminals is low

The Cyber Related Fraud Problem

4.7m
reported Business Cybercrimes in 2017 (+67%)

£1.1Bn
Reported fraud and computer misuse incidents in UK ONS - 2015/16

68%
Year on Year rise in reported crime

Only 20%
Organisations have performed a Fraud Risk Assessment

47,000
Reports each month to UK ActionFraud

9
Different organisations measuring fraud in the UK

57
cybercrime prosecutions in 2016

£160m
by a single fraud ring currently in court:
75 solicitors avg $2.1m

1,300%
Rise in the last 18 months in reported Email Scams, FBI

£160m
a single fraud from healthcare provider

US$3.1Bn
Lost to scams in last 18 months, FBI, %

£113m
Cold!
Losses to a single scam in 2016

Cifas members (350 financials) – Fraud +16% in 2016/17

Fraudsters claiming to be from ActionFraud

IT Pro
NFIB & GetSafeOnline
ActionFraud
Intel from STORM

FTC
BBC
ONS
PwC

STORM Guidance
Assess | Plan | Respond

The Cyber Related Fraud Problem

Smishing Scams

Victims manipulated via SMS messages where fraudsters pretend to be victims Bank, telecoms operators, gaming providers – Sometimes supported by email

Govt. Impersonation

Commonwealth Card, Tax Refund, Death Duties, ICO fees, Good Citizen Award, Council Tax, debt collection, Student loans

Conveyancing scams

Faking IDs of Solictors, Buyers/ Sellers, Agents, Lenders

Public Wifi interception

Vishing Scams

Victims manipulated via telephone calls where fraudsters pretend to be victims Bank, the Police or a counterparty Solicitor – Sometimes supported by email

Fake Goods, Services & Rent Deposits

Ebay, Amazon, Gumtree, Property Agents, Delivery (Royal Mail/DHL Fedex, Fake Gift Cards, Cars, Drones

Poison Bills

Fake utility bills, invoices and receipts delivering malware

Ransomware & Hacking/ DDoS Extortion

Fake Investments

Investment scams enticing victims to invest in a range of false assets including wine, antiques & art and property as well as offshore pensions.
Money Laundering scams

Whaling

Fake boss scams

Pharming

Fake websites with URLs similar to legitimate sites

Package Delivery Scams

Telecomms Scams

Fixed line & Mobile phone – mostly premium rate frauds Business directory frauds Malware installs Phone Upgrade Scams

Recovery Room

Fraudsters offering to recover funds from prev victims

PII misuse

to target Mental Health Patients and the Elderly

Package undelivered/ seized

Online Ticket Scams

55% increase in 2015/16.
Sport, Theatre and Religious events, Holidays, Lottery

Online Gaming Scams

Malware downloads, unlimited faming, fake deposits

Heartbreak

Online dating accounts for 27m losses – 2 out of 3 romance frauds

Scamming Signatures on Doorsteps & Fake mailboxes

STORM Guidance
Assess | Plan | Respond

Value in technology…In order of importance

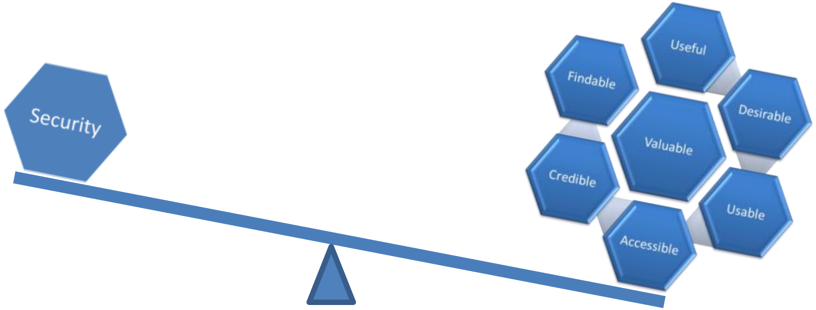
In the digital world…

“Utility trumps Security”

Organisations are driven by a take-up in technology which rarely properly considers business and technology risk. This means that security has to be retro-fitted after solutions are adopted.

Example

Webmail without 2-Factor Authentication



Who are the Threat Actors?

- Organised Criminals
  - Fraud & Extortion rings: Pop=V.High, Cap=Med.High
  - Data brokers: Pop=Med.High, Cap=Med
- Nation State Sponsored (govt. staff & contractors): Pop=Low, Cap=V.High
- Activists: Pop=Low, Cap=Med.High
- Insiders
  - Disgruntled employees: Pop=Med, Cap=High
  - Fraudsters: Pop=Med, Cap=High
- Lone hackers (skilled): Pop=Low, Cap=V.High
- Lone hackers (scripties) : Pop=Med, Cap=Med

Population estimates determined as those likely to act on a general commercial business

201x-The Decade of the Fraudster!

Consumer Scamming
Personal ID Theft

Capital Scams

Working for Delhi's fraud call centres

THANG[illegible]O HAOKIP | 1 October 2013

ERIC FOR THE CARAVAN

A fraud call centre in north-west Delhi. The Delhi Police claims there are more than 10,000 such outfits in the city.

Law Enforcement
largely ineffective

Business Scamming
Organisation ID Theft

Spike in Fraud Attempts

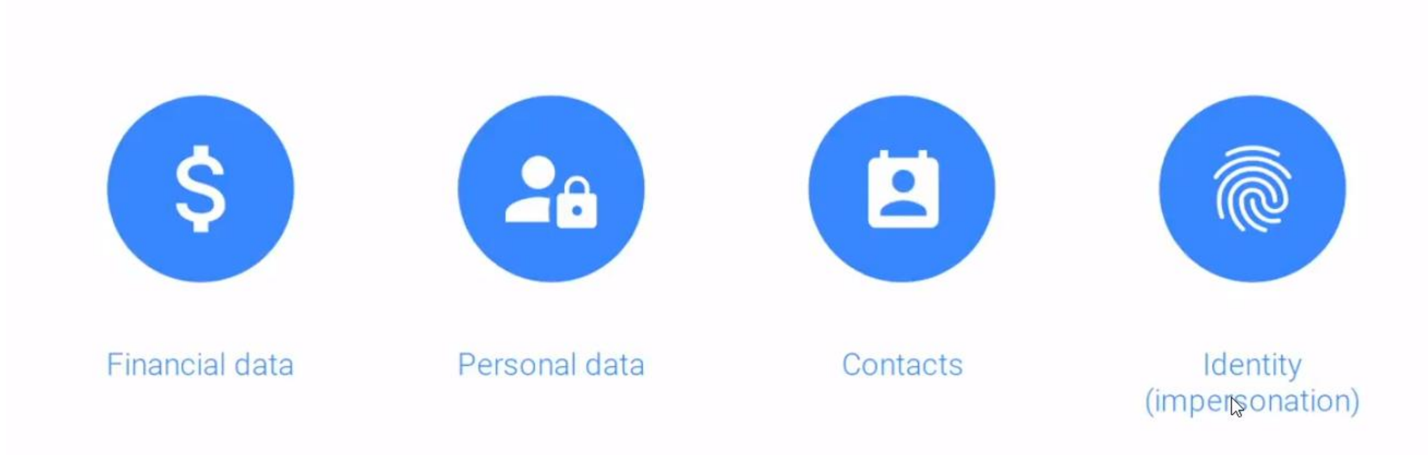
- Phishing via email

  Using spoofed email names some domain others via yahoo/web mail
- Mailbox hijacking
- Latest attacks: Advanced Malware

  Hijacking online banking sessions
- Awareness is Key
- Multi-Factor Authentication a **Must**
- Email <u>not</u> suitable for business: use secure web portals

Mailbox Hijacking

Valuable data in mailboxes – easily accessible online!



Mailbox Hijacking

Three main methods used to steal credentials to hijack mailboxes

>3.3Bn

>1M

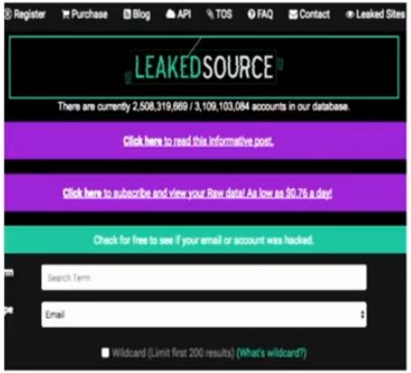
>12M

2016 Losses

2018 Losses X20

Mailbox Hijacking

The marketplace



There are currently 2,508,319,669 / 3,109,103,084 accounts in our database.

Click here to read this informative post.

Click here to subscribe and view your Raw data! As low as $0.76 a day!

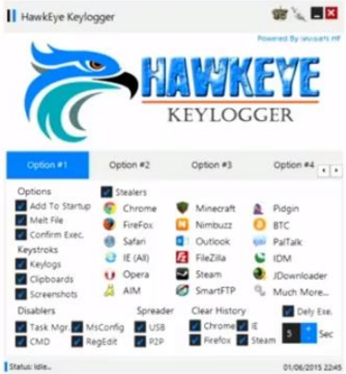
Check for free to see if your email or account was hacked.

Search Term

Email

□ Wildcard (Limit first 200 results) (What's wildcard?)

Data breach market



Options
☑ Add To Startup
☑ Melt File
☑ Confirm Exec.

Keystroks
☑ Keylogs
☑ Clipboards
☑ Screenshots

☑ Stealers
Chrome, FireFox, Safari, IE (All), Opera, AIM, Minecraft, Nimbuzz, Outlook, FileZilla, Steam, SmartFTP, Pidgin, BTC, PalTalk, IDM, JDownloader, Much More...

Disablers
☑ Task Mgr. ☑ MsConfig
☑ CMD ☑ RegEdit

Spreader
☑ USB
☑ P2P

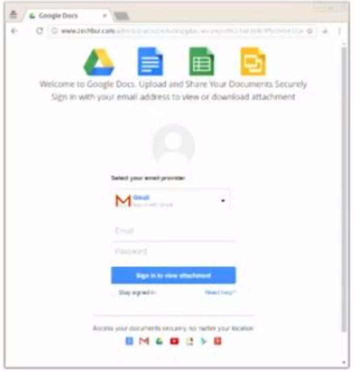
Clear History
☑ Chrome ☑ IE
☑ Firefox ☑ Steam

☑ Dely Exe.
5 Sec

Status: Idle...

01/06/2015 22:45

Keyloggers



Welcome to Google Docs. Upload and Share Your Documents Securely

Sign in with your email address to view or download attachment

Select your email provider

Email

Password

Access your documents securely, no matter your location

Phishing kits

Mailbox Hijacking

The marketplace

Google collected over 4000 data breach dumps with over 3.3Bn credentials

67 Million Unique Google credentials

Mailbox Hijacking

The marketplace

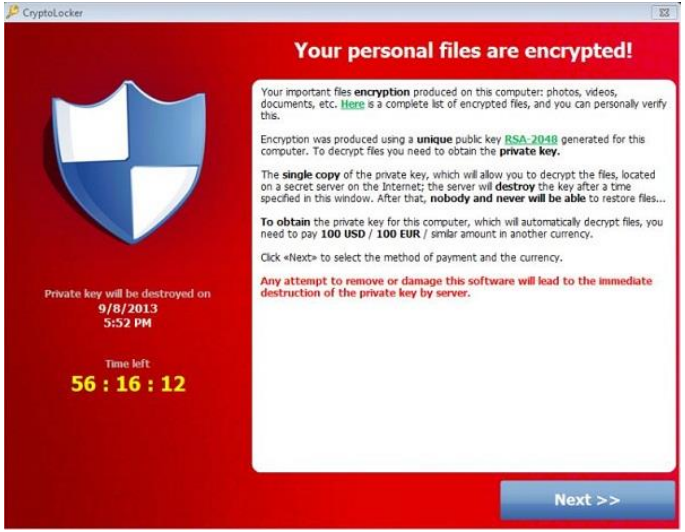
Password reuse

12-47%*

**Google Data Breaches, Phishing & Malware Survey*

Ransomware Epidemic

- Hit a number of businesses
  UK NHS, Maersk Shipping, but…
  Biggest impact on SMEs
- Paying ransom never a good idea
- Decryption unreliable



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD** / **100 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

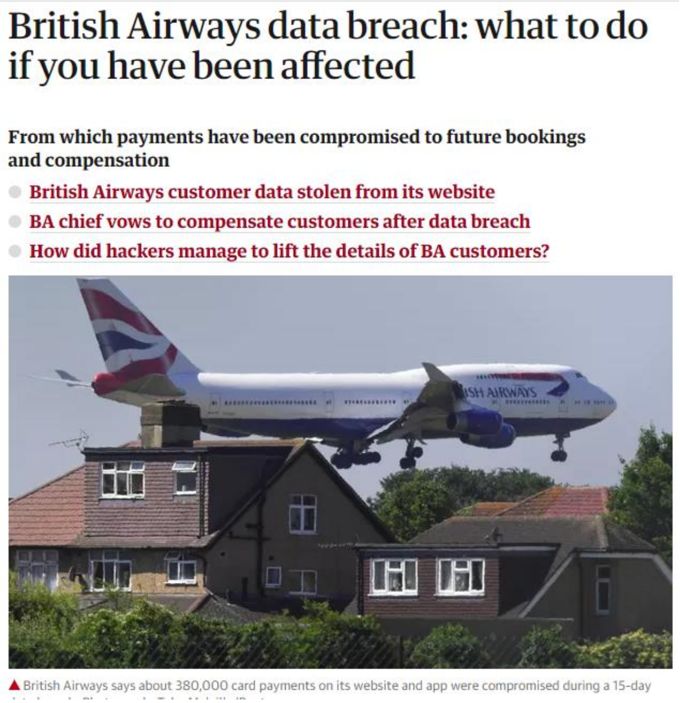
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
9/8/2013
5:52 PM

Time left
56 : 16 : 12

Breach News Continues: Almost Daily

- How <u>not</u> to manage a breach
  - Third data breach in 12 months
  - Bad PR
    - BBC: “Was breached data encrypted?”
    - Harding: “I don’t know”
  - Hi-tech Advanced Persistent Threat attack by state-sponsored experts?? No: All arrested were under 21
  - Spin: Exploit really complex
  - Reality: standard SQL injection – v. poor security
- How <u>not</u> to manage a breach V2
  - Cost over $400m, ICO max fine - £500k
- How <u>not</u> to manage a breach V3
  - Third major tech. problem in 12 months
  - Spin: Exploit really complex
  - Reality: standard CMS code injection/frame overlay
  - Fix available for over a year



British Airways data breach: what to do if you have been affected

From which payments have been compromised to future bookings and compensation

- **British Airways customer data stolen from its website**
- **BA chief vows to compensate customers after data breach**
- **How did hackers manage to lift the details of BA customers?**

▲ British Airways says about 380,000 card payments on its website and app were compromised during a 15-day

STORM Guidance
Assess | Plan | Respond

The Need for Cyber Risk Assessment

Most Insureds <u>do not</u> manage cyber risk

- Insurers need to use effective methods to determine risk
- Appreciating the insureds internal ‘organisational’ challenges!

Insureds supply chains are becoming more complex

- Inter-dependencies need to be assessed & understood
- Opportunity to offer to insure entire chains!

Systemic risk triggers appear to be more likely

- Business interruption losses may be considerable
- Risk is proportional to the speed of automation & common tech/support vendors

Cyber Risk Assessment Options

Three general approaches for assessment on offer

1. In-depth, Arm's Length Questionnaire type – send client a form (trad or online)
   - Extensive Q&A ; built into prop form. Risks inaccurate & contrived answers and delay
   - Low cost

2. In-depth risk assessment by specialists: usually with client on-site
   - Quality enquiry likely to give accurate result, time consuming and intensive on client
   - Clients will appreciate but expensive & means can only apply to high-end business

3. Open source intel gathering or extremely pared-down question set
   - Low or zero impact on client, incomplete risk picture
   - Less expensive

Cyber Risk Assessment Options

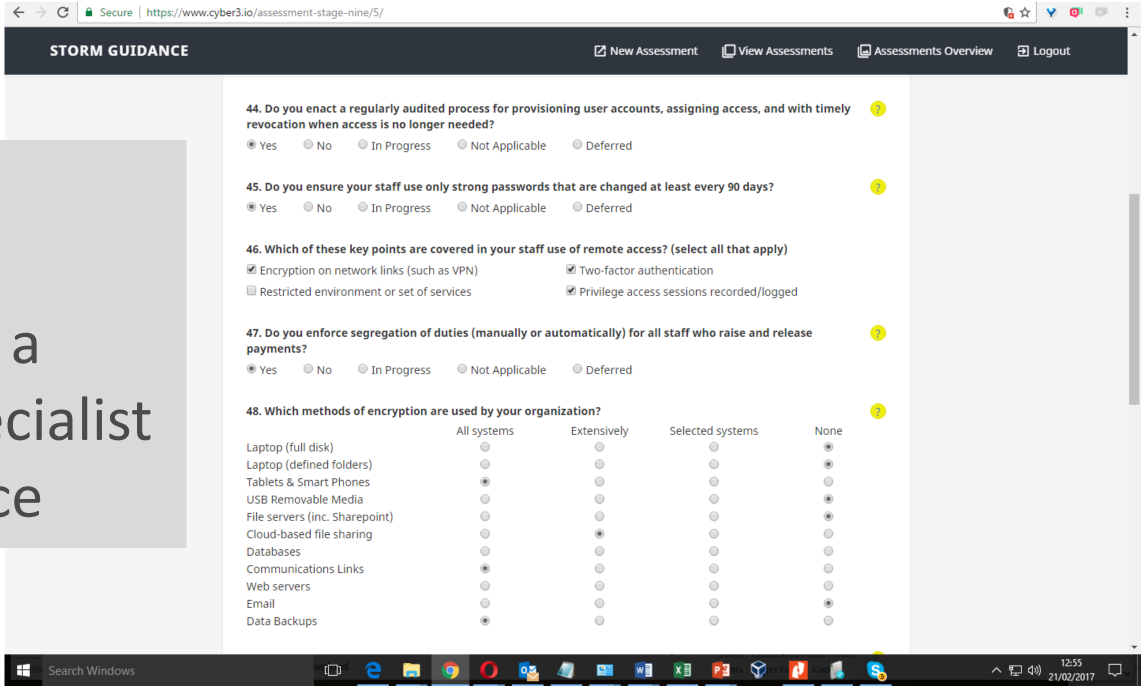
Fourth Approach

Comprehensive questions set: complete cyber risk picture & sector-specific modules

- Extensive Q&A ; delivered via specialist-driven online questionnaire over web conference
- Costs low enough to be applied to all levels of business and the entire book
- Can be pre or post-bind and as a subjectivity or 'value-add'
- Quality enquiry likely to give accurate result, not time consuming and intensive on client
- Clients appreciate specialist involvement and advice
- Generate consistent reporting that pivots on repeatable Key Risk Indicators (KRIs)
- Designed to promote virtuous cycle of improvement in controls; ongoing relationship & encouraging client loyalty

Our 4th Approach: CYBER3 - Rapid Risk Review

Secure online questionnaire walkthrough with a STORM Cyber Specialist via web conference



44. Do you enact a regularly audited process for provisioning user accounts, assigning access, and with timely revocation when access is no longer needed?

● Yes ○ No ○ In Progress ○ Not Applicable ○ Deferred

45. Do you ensure your staff use only strong passwords that are changed at least every 90 days?

● Yes ○ No ○ In Progress ○ Not Applicable ○ Deferred

46. Which of these key points are covered in your staff use of remote access? (select all that apply)

☑ Encryption on network links (such as VPN)
☑ Two-factor authentication
□ Restricted environment or set of services
☑ Privilege access sessions recorded/logged

47. Do you enforce segregation of duties (manually or automatically) for all staff who raise and release payments?

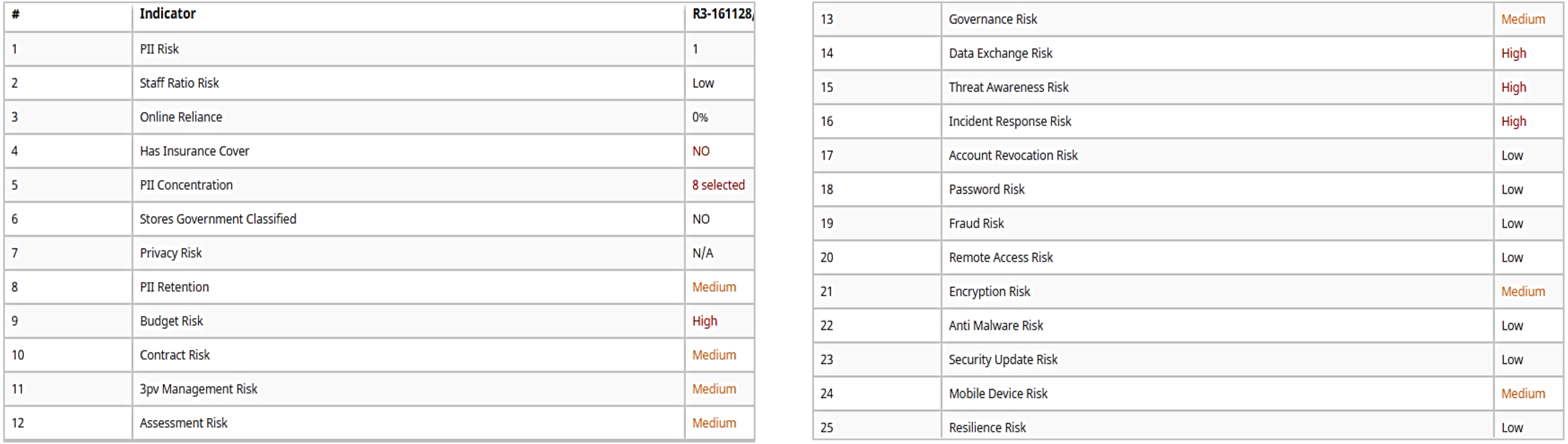
● Yes ○ No ○ In Progress ○ Not Applicable ○ Deferred

48. Which methods of encryption are used by your organization?

	All systems	Extensively	Selected systems	None
Laptop (full disk)	○	○	○	●
Laptop (defined folders)	○	○	○	●
Tablets & Smart Phones	●	○	○	○
USB Removable Media	○	○	○	●
File servers (inc. Sharepoint)	○	○	○	●
Cloud-based file sharing	○	●	○	○
Databases	○	○	○	○
Communications Links	●	○	○	○
Web servers	○	○	○	○
Email	○	○	○	●
Data Backups	●	○	○	○

Our 4th Approach: CYBER3 - Rapid Risk Review

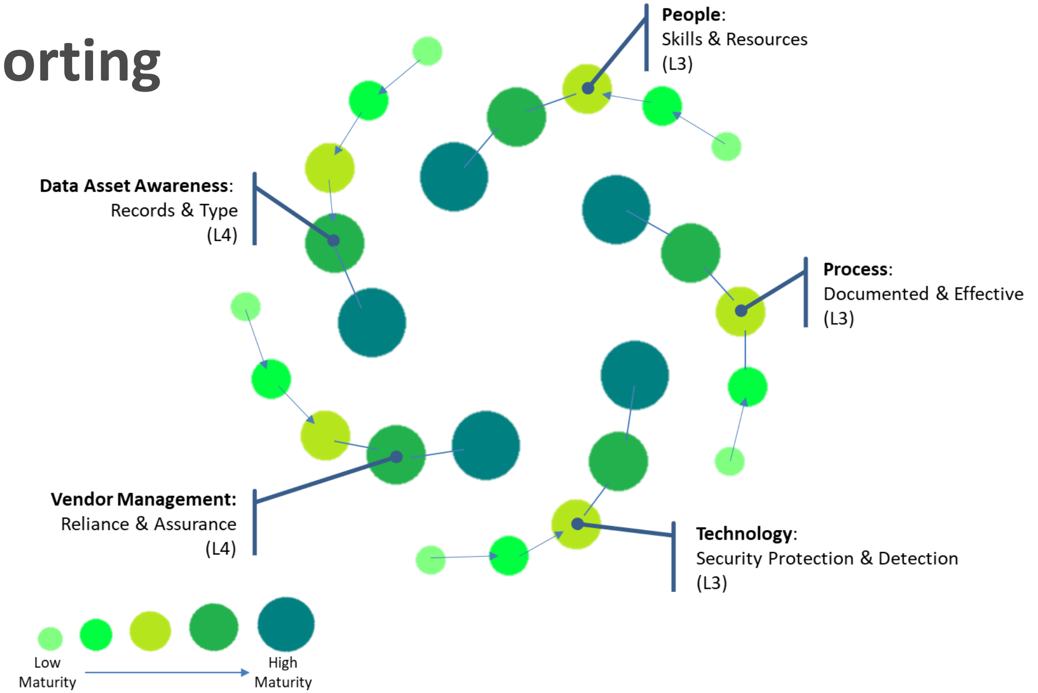
Graphical Reporting



#	Indicator	R3-161128,
1	PII Risk	1
2	Staff Ratio Risk	Low
3	Online Reliance	0%
4	Has Insurance Cover	NO
5	PII Concentration	8 selected
6	Stores Government Classified	NO
7	Privacy Risk	N/A
8	PII Retention	Medium
9	Budget Risk	High
10	Contract Risk	Medium
11	3pv Management Risk	Medium
12	Assessment Risk	Medium
13	Governance Risk	Medium
14	Data Exchange Risk	High
15	Threat Awareness Risk	High
16	Incident Response Risk	High
17	Account Revocation Risk	Low
18	Password Risk	Low
19	Fraud Risk	Low
20	Remote Access Risk	Low
21	Encryption Risk	Medium
22	Anti Malware Risk	Low
23	Security Update Risk	Low
24	Mobile Device Risk	Medium
25	Resilience Risk	Low

CYBER3 Highlights

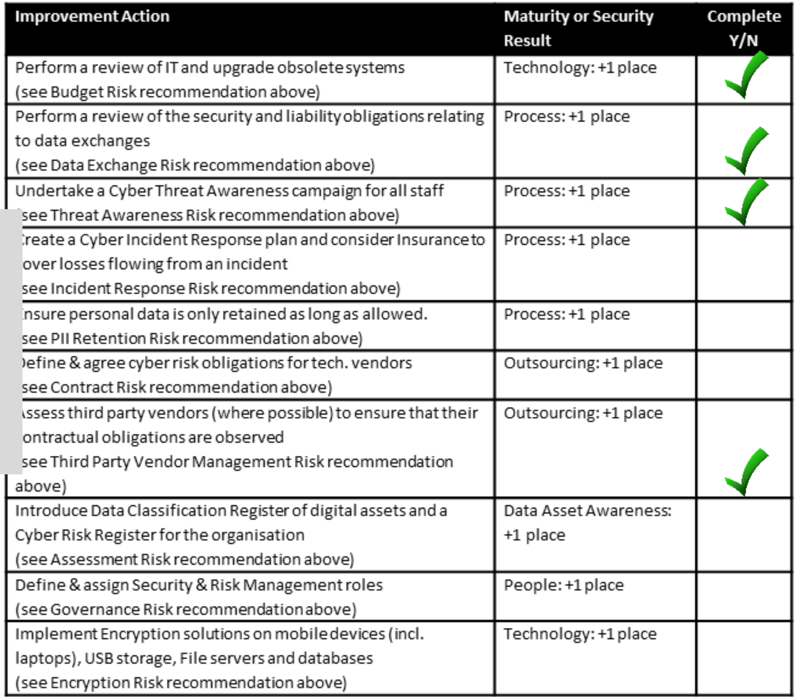
Graphical Reporting



STORM Guidance
Assess | Plan | Respond

Supporting a Continuous Improvement Cycle

Top-10 Cyber Improvements Checklist

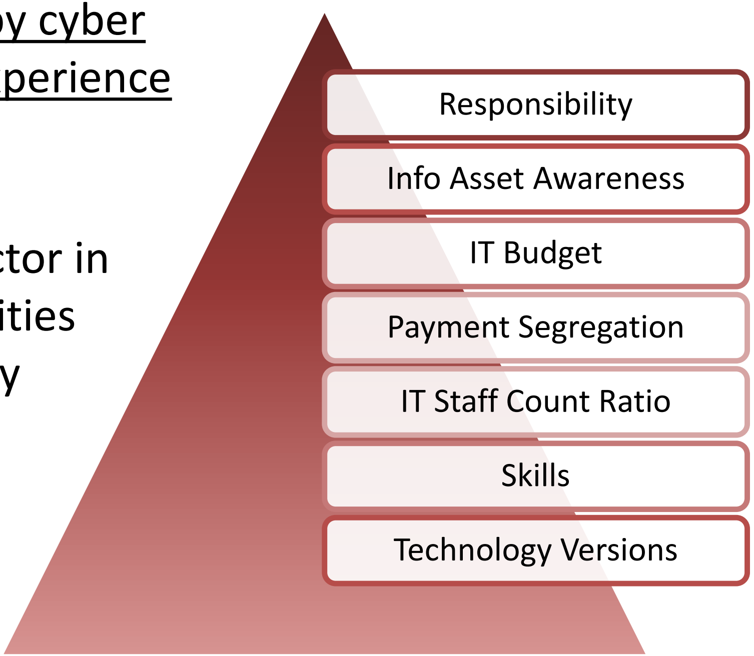


Improvement Action	Maturity or Security Result	Complete Y/N
Perform a review of IT and upgrade obsolete systems (see Budget Risk recommendation above)	Technology: +1 place	✓
Perform a review of the security and liability obligations relating to data exchanges (see Data Exchange Risk recommendation above)	Process: +1 place	✓
Undertake a Cyber Threat Awareness campaign for all staff see Threat Awareness Risk recommendation above)	Process: +1 place	✓
reate a Cyber Incident Response plan and consider Insurance to over losses flowing from an incident see Incident Response Risk recommendation above)	Process: +1 place	
nsure personal data is only retained as long as allowed. see PII Retention Risk recommendation above)	Process: +1 place	
efine & agree cyber risk obligations for tech. vendors see Contract Risk recommendation above)	Outsourcing: +1 place	
ssess third party vendors (where possible) to ensure that their ontractual obligations are observed see Third Party Vendor Management Risk recommendation above)	Outsourcing: +1 place	✓
Introduce Data Classification Register of digital assets and a Cyber Risk Register for the organisation (see Assessment Risk recommendation above)	Data Asset Awareness: +1 place	
Define & assign Security & Risk Management roles (see Governance Risk recommendation above)	People: +1 place	
Implement Encryption solutions on mobile devices (incl. laptops), USB storage, File servers and databases (see Encryption Risk recommendation above)	Technology: +1 place	

Cyber Risk Indicators: *Seven Deadly Cyber Sins*

Informed by cyber incident experience

Need to factor in the capabilities delivered by vendors



Responsibility

Info Asset Awareness

IT Budget

Payment Segregation

IT Staff Count Ratio

Skills

Technology Versions

High Risk?

No Board-level owner

No Info Asset Register

Less than 7% of revenue

Raise & Release by same person

Less than 5% of end users

No Formal InfoSec/Response Skills

Older than Previous

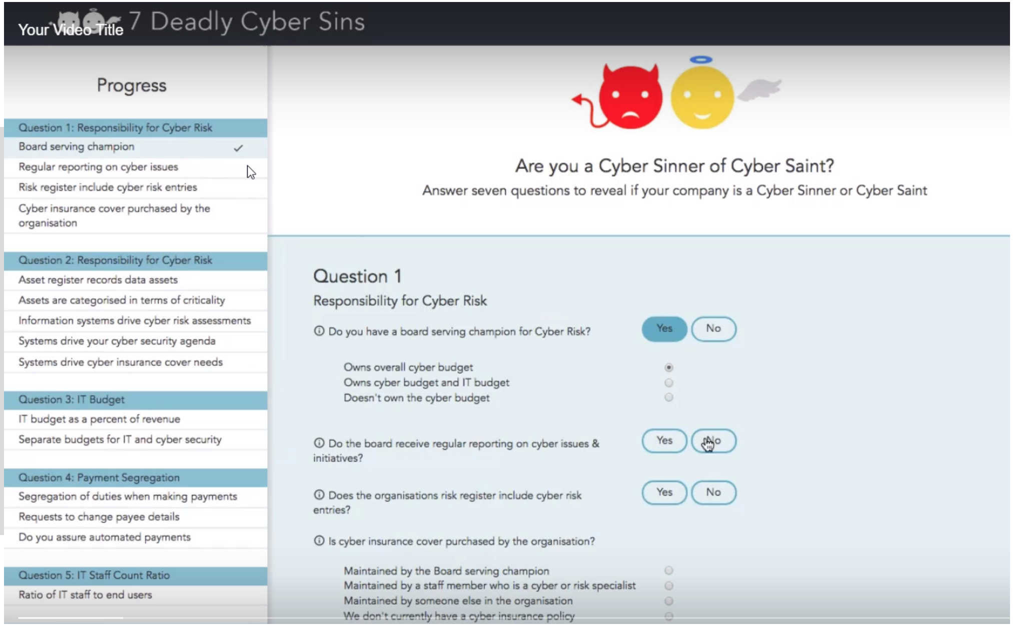
7 Deadly Cyber Sins: Self-Assessment

Secure online self-assess

Result: Cyber Saint or Sinner

Saint=Certificate & Voucher

Sinner=Remediation Plan



Progress

Question 1: Responsibility for Cyber Risk
- Board serving champion ✓
- Regular reporting on cyber issues
- Risk register include cyber risk entries
- Cyber insurance cover purchased by the organisation

Question 2: Responsibility for Cyber Risk
- Asset register records data assets
- Assets are categorised in terms of criticality
- Information systems drive cyber risk assessments
- Systems drive your cyber security agenda
- Systems drive cyber insurance cover needs

Question 3: IT Budget
- IT budget as a percent of revenue
- Separate budgets for IT and cyber security

Question 4: Payment Segregation
- Segregation of duties when making payments
- Requests to change payee details
- Do you assure automated payments

Question 5: IT Staff Count Ratio
- Ratio of IT staff to end users

Are you a Cyber Sinner of Cyber Saint?

Answer seven questions to reveal if your company is a Cyber Sinner or Cyber Saint

Question 1

Responsibility for Cyber Risk

ⓘ Do you have a board serving champion for Cyber Risk? [✓ Yes] No

- Owns overall cyber budget ●
- Owns cyber budget and IT budget ○
- Doesn't own the cyber budget ○

ⓘ Do the board receive regular reporting on cyber issues & initiatives? Yes No

ⓘ Does the organisations risk register include cyber risk entries? Yes No

ⓘ Is cyber insurance cover purchased by the organisation?

- Maintained by the Board serving champion ○
- Maintained by a staff member who is a cyber or risk specialist ○
- Maintained by someone else in the organisation ○
- We don't currently have a cyber insurance policy ○

Future Predictions

How Will Cyber Risk Develop?

Interesting times ahead...

- 1-2 years
    - GDPR is changing the privacy liability and legal risk & drive extortion
        - Already driving more incident reports/claims
    - BI exposure & losses will continue to grow
- 3-4 years
    - Legacy embedded systems will result in new risks i.e. health & safety
    - Systemic risks more prevalent
- 5-10 years
    - Higher costs on security management i.e. encryption services
    - Crypto-currency adoption will drive new security needs, fraud may drop

How Will Cyber Insurance Develop?

Interesting times ahead…

- Significant market growth
  - GDPR already driving more need for cover in liability & response costs
  - Need for improved benchmarking and comparison
  - Integration of cyber risk cover into traditional lines
  - Quantification methods in cyber incidents to improve loss adjustment
  - Pooling to manage systemic risk
  - Better risk assessment methods and supply chain cover offers
  - Problems with US approaches incl. conflicts of interest
  - Improvements in claims management
  - Insurance will play significant role in improving cyber resilience

Systemic Cyber Risk

In the digital world…

…An organisations security is only as strong as its’ most vulnerable supplier

STORM Guidance

Strategic, Tactical & Operational Risk Management

Thank you

Neil Hare-Brown MSc CISA CISSP CITP MBCS

CEO