

# Improving your Rumsfeld score – by reducing your unknown unknowns

---

Tim Rawlins - Director & Senior Adviser



# Tim Rawlins - Director & Senior Adviser





**What  
do  
they  
want?**






















## Cyber and geo-political threats continue to blend

---

**Active Adversaries** constantly develop new attacks so you must constantly adapt at all levels of **people, process and technology** to defend against:

- Sophisticated **organised crime gangs** focused on **data theft** and **ransomware** for money, and using your data to target clients and supply chain for further attacks, along with '**business email compromise**' – fraud and diverting money to different accounts
- Other **individuals and gangs** looking to **steal money, data, intellectual property** and **cause disruption** for business impact, fun, potentially targeting you for bragging rights or to make a political point
- **Hostile state intelligence organisations** for **data collection** on individuals, **commercial IP, training AI**, and **positioning to support disruptive action**

# The proliferation of ransomware and data theft gangs continues

 <b>RansomHub</b> Last active: 11th Jul 2024 11:51 Total Victims: 153	 <b>Cactus</b> Last active: 11th Jul 2024 08:27 Total Victims: 144	 <b>ClOp</b> Last active: 11th Jul 2024 07:39 Total Victims: 555	 <b>Play</b> Last active: 11th Jul 2024 00:00 Total Victims: 509	 <b>BlackSuit</b> Last active: 10th Jul 2024 17:12 Total Victims: 95
 <b>Cloak</b> Last active: 10th Jul 2024 11:19 Total Victims: 46	 <b>HuntersInternational</b> Last active: 10th Jul 2024 06:28 Total Victims: 136	 <b>Akira</b> Last active: 10th Jul 2024 00:00 Total Victims: 320	 <b>Monti</b> Last active: 9th Jul 2024 20:07 Total Victims: 52	 <b>Medusa</b> Last active: 8th Jul 2024 10:29 Total Victims: 269
 <b>DragonForce</b> Last active: 8th Jul 2024 00:00 Total Victims: 74	 <b>Abyss</b> Last active: 7th Jul 2024 13:25 Total Victims: 44	 <b>Rhysida</b> Last active: 7th Jul 2024 06:51 Total Victims: 103	 <b>IncRansom</b> Last active: 5th Jul 2024 19:37 Total Victims: 195	 <b>SpaceBears</b> Last active: 5th Jul 2024 01:53 Total Victims: 21

# Cyber Value-at-Risk per asset calculation

---

$$CVaR_i = t_i * (c_i * (a_i + \sum_{i=1}^N (\pi^i h; ) * v_i))$$

where:

- t = probability of a threat occurring
- c = probability of a control being effective
- a = value (to replace) of the asset
- h,v = harm probability and value from an ordered set of harms H
- i = each i is a different simulation



# Rumsfeld Score of Cyber Resilience

---

$$Rs = \frac{[kA + uA]sD^{\gamma} * (u \uparrow \tau * kV + uV) - u\beta}{i + [(uR^3) * uCMT + uS]}$$

Where

k = known knowns

u = unknown unknowns

A = Assets and Important Business Services

$\uparrow \tau$  = ever increasing threats

sD = Security Debt

V = Vulnerabilities

$\beta$  = Back-ups

i = investment











R = Ransom, Reputation, Regulatory fines

CMT = Crisis management training at Gold, Silver and Bronze levels

S = stakeholders

*This is a joke NOT  
a real formula*

# Current and Future Technical Challenges for Resilience

-  DDoS attacks increasing with attack resources rented for less than £10 an hour
-  You almost definitely aren't following your data retention policies
-  Business Email Compromise makes more money than ransomware attacks
-  Ransomware attacks are blended with theft of staff, client, corporate data
-  Dwell times from hours to months as they attack, sell access, or watch your activities
-  Back-ups are vulnerable to encryption, downsizing or deletion
-  Multi-cloud environments and AI are a challenge to manage securely with privacy
-  Post quantum computing will see your encryption challenged
-  Increasing regulation is demanding focus on your and your supply chain's resilience
-  Deepfakes will challenge training and processes in KYC, HR, Security & Operations



# Crisis Management - the Gold, Silver, Bronze model



Resilience: effective recovery is far longer than your BCM plans says

---

**4 Days**

Understand the incident

Initial action to reduce risk and block the attackers' access.

Identifying the initial attack vector may take several days

**4 weeks**

Identify the impact

Recovering data will require immediate remediation work to secure, rebuild, and assure the environment before you start data recovery activities

**4 months**

Manage stakeholders

Reconnecting with your external stakeholders will take longer to manage and require more effort than you imagine



# Decisions required – IT priorities in a crisis

## Re-establish Infrastructure

Forensic capture  
of data

Identifying  
backups

Replacing IT  
equipment

Restoring control  
applications



## Regulatory, Legal or Statutory Demands

Reporting capabilities

Contractual obligations



## Wider Business Activities

Underlying  
applications

Business  
Operations

Data  
recovery and  
storage

Staff & Client  
support

Operational  
Technology

Data sharing  
stakeholders

# Resilience – our lessons learnt from multiple crises

A crisis is bad news; not all bad news is a crisis

A crisis is not 'business as usual' and so demands agility and a pivot in concurrent activity

**Be prepared for an escalating crisis over the long term**

In the face of chaos, **you can only control your message**, so get it right every time

All audiences are connected; **your internal audience is as critical as any external audience**

Silos are stupid – but “need to know” still exists along with legal privilege

Be compassionate and calm – everyone is watching you

Your perspective will depend on the available intelligence

Deal with the ambiguity and make decisions anyway

Challenge your narrative and drive it with data to improve your response

**Map and track your stakeholders - they will take ages to manage**

**Make friends when you don't need them**



**Remember,** it's when not if.  
Hope is not a strategy.



# Improving your Rumsfeld score – by reducing your unknown unknowns

---

Tim Rawlins - Director & Senior Adviser