Cyber Security Governance: Updates from the front line, October 2022

Latest Cyber Threat Evolution

Introduction

Neil Hare-Brown
Cyber Jedi

- Founder: STORM Guidance: niche independent cyber advisory
- Information Security & Digital Investigator for 35 years: Financial Services, Government/Law Enforcement, Military, Industry, Retail, Marine
- Alumni Royal Holloway: MSc. Information Security
- Specialisms:
  - Cyber Risk: Assessments & Audits
  - Cyber Incident Response: Digital & Fraud Investigations and
  - Cyber Crisis Mgmt.
  - Cyber Insurance: Worked with cyber insurers & brokers exclusively for 8 years
- Current Assignments: 100's of Cyber & Fraud Investigations, Rapid Risk Reviews, IR Plans, **CyberDecider** & **ReSecure**

STORM Guidance

Full service offering for reinsurers, insurers, brokers and clients

Assess

Lightweight cyber risk assessments to enable clients to learn and improve their cyber risk management maturity levels. **Cyber3: Rapid Risk Review**

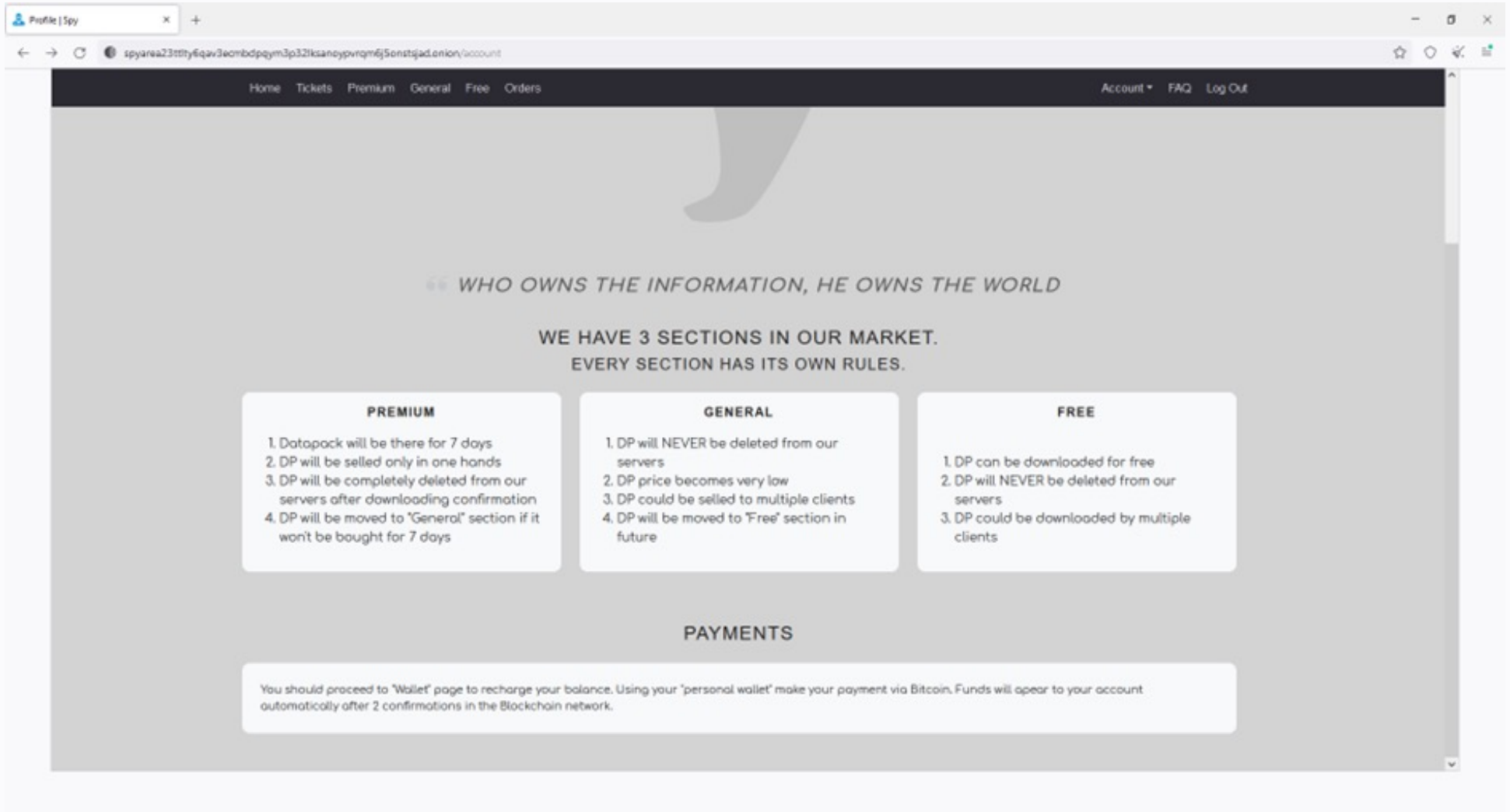
Plan

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.

Respond

Delivering a fully coordinated and Integrated Cyber Incident Response Team (I-CIRT).

ReSecure: full service offering for insured clients.


Profile | Spy
spyarea23tttty6qav3ecmbdpqym3p32lksanoypvrqm6j5onstsjad.onion/account
Home Tickets Premium General Free Orders
Account FAQ Log Out
WHO OWNS THE INFORMATION, HE OWNS THE WORLD
WE HAVE 3 SECTIONS IN OUR MARKET.
EVERY SECTION HAS ITS OWN RULES.
PREMIUM
1. Datapack will be there for 7 days
2. DP will be selled only in one hands
3. DP will be completely deleted from our servers after downloading confirmation
4. DP will be moved to "General" section if it won't be bought for 7 days
GENERAL
1. DP will NEVER be deleted from our servers
2. DP price becomes very low
3. DP could be selled to multiple clients
4. DP will be moved to "Free" section in future
FREE
1. DP can be downloaded for free
2. DP will NEVER be deleted from our servers
3. DP could be downloaded by multiple clients
PAYMENTS
You should proceed to "Wallet" page to recharge your balance. Using your "personal wallet" make your payment via Bitcoin. Funds will apear to your account automatically after 2 confirmations in the Blockchain network.

Ransomware

Evolving Threat

- Gone from pure network disruption to pure data extortion
- Criminal 'Threat Actors ' have evolved attacks to maximise probability of payouts
  - Businesses are gradually improving resilience to Ransomware attacks and so are less likely to need to pay to recover their systems
  - Most businesses remain largely ignorant of the sensitivity of the data they hold
  - TAs are more likely to obtain extortion demand payouts because of Reputational/Liability risk from data breaches
  - Dark web marketplaces are becoming optimised for data breach extortion
  - Any data theft is now more likely to follow a 'ransomware-style' extortion process

Safeguard

Ransomware/Data Breach

- People – Process – Technology

  Focus has been on Technology and on People. It now needs to be firmly on Process as this is where Threat Actors are focused.

- Know your data

  Undertake a proactive audit to discover sensitive business data

  Improve data management and security e.g. encryption

- Build CIR plans (even 'plan-on-a-page) and perform exercises on realistic incident scenarios

- Consider Threat Actor Engagement as an important aspect of your plans

Critical National Infrastructure Attack Fallout

Evolving Threat

- War appears to attenuate criminal activity
- However, it is a period where development of attack capability is generally high
  - Nation-state cyber capabilities currently focus on controlled disruption of CNI
  - Post-conflict, those capabilities will inevitably make their way into the hands of cyber criminals
- Both CNI and non-CNI organisations need to be prepared for the use of increased disruptive attacks and extortion
- There may be further uncertainty as to how War Exclusions will be triggered
- Disinformation and fraud scams are continuing to develop rapidly – again Process

Safeguard

Increased Cyber Attacks

- Critical for organisations (CI or not) to understand their Cyber Risk Management Maturity (CRMM).
  - Undertake a comprehensive cyber risk assessment
- Adopt a strategic plan for cyber risk management
  - **Do not just expect the IT folks to keep the wolves from the door**
- Improve your spend on IT and cyber security
  - Focus on improving process in the procurement and support of technology and digital services
  - Ensure that ALL technologies are at the latest available versions

Challenge #1

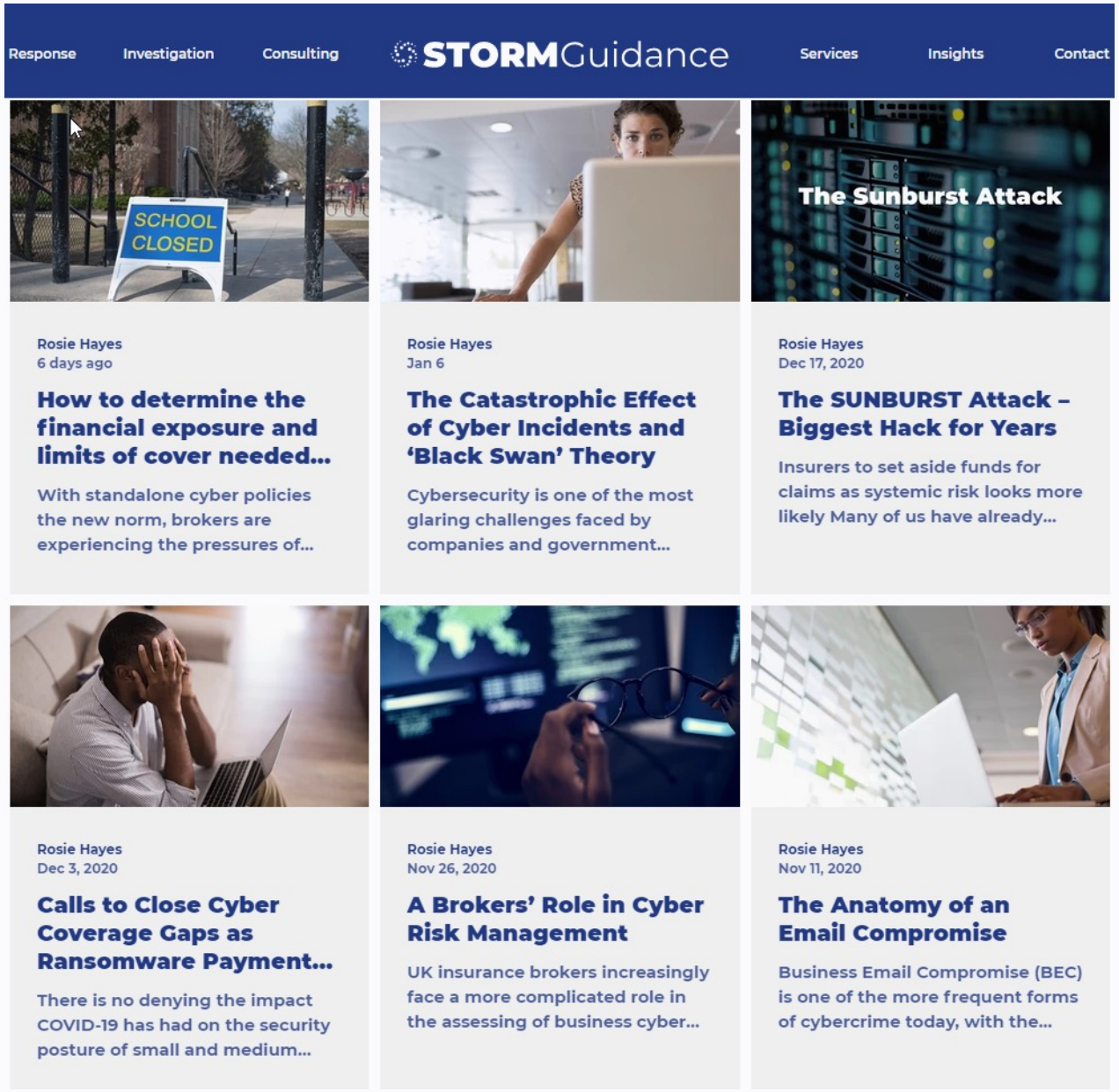
Have a Strategy

Tactics without strategy is the noise before defeat

Sun Tzu – The Art of War

Supporting Information

www.stormguidance.com/insights



STORMGuidance

Thank you

contact@stormguidance.com