Organizations in 2018...

...now collect and are store more data than ever...

... in more places than they’ve ever had it.

Creating a “follow the data” problem
Follow the Data...

All this **data** needs to be:

- Created / Collected
- Stored
- Controlled
- Destroyed

... **SECURELY**

---

Follow the Data...

- The human and **financial costs** of creating, storing, destroying and following this data are greater than they have ever been
- Increased **threat sophistication** and persistence targeting data, exposing **weaknesses** in data security infrastructure and processes
- Movement toward cloud infrastructure **simplifies IT**, while complicating the problem
- This **evolving data footprint** is compounded by numerous **evolution** trends in cybercrime
Evolution...

Infrastructure  Attacks  Cyber-Capitalization  Countermeasures  Regulatory Climate

The Expanding Network
Direct Connect Creates Expanded Networks to Protect
Evolution... of Attacks

Infrastructure
(DDoS, Websites, Networks)

Data
(Database Dumps, Destruction, Disclosure)

Individual
(Identity Theft, Spear Phishing)

Multi-Phased and Multi-Staged Attacks
Evolution... of Capitalization

- Financial
- Intellectual
- Political
- Personal / Human

Evolution... of Countermeasures

- Tools
- Human-based
  - Eyes on glass
  - SOCS
- Modern
  - Intelligence
  - Analytics/Big Data
  - AI
Evolution... of Regulatory Climate

Breaches  •  Lawsuits  •  Legislation (GDPR, DPA)  •  Trial by social media

Less Money, More Problems

• Rising IT and data centre costs
• Rare and expensive IT Security personnel
  • Training Costs
  • Certification Costs
  • Turnover
• Push to Cloud / MSP
• Increased threat sophistication and persistence targeting data, exposing weaknesses in data security infrastructure and processes
Gartner’s experience is that many organizations simply do not know their security budget. This is partly because few cost accounting systems break out security as a separate line item, and many security-relevant processes are carried out by staff who are not devoted full-time to security, making it impossible to accurately account for security personnel. In most instances, the chief information security officer (CISO) does not have insight into security spending throughout the enterprise.

The Paradox

More threats
More data
More complex data footprint
More regulation
Less budget
Less staff
Less time

How do organizations succeed?
Accept the Paradox

- Accept Cybersecurity in the executive boardroom
- Accept the inevitability of failure
  - Explore Cyber-Armageddon
  - Have appropriate response plans/teams
  - Red team/Executive table-top
- Accept the adversary is formidable
- Intelligence – Consume only what you understand
- Outsource carefully and appropriately
  - Understand the (shared) responsibility
  - Understand the output
  - Augment your team and abilities – not replace

Thank you!

Ajay K. Sood
@akssecure