

# Understanding & managing risk across your digital infrastructure



*Ali Neil*

*Director of International Security Solutions*

*Verizon*



# Understanding & Managing Risk Across Your Digital Infrastructure

Ali Neil

Director Security Solutions

16<sup>th</sup> of May

verizon

---

# 2019 DBIR - Main Takeaways

- C-level executives increasingly and proactively targeted by social breaches. 9X more likely to be victim of social breach than previously.
- Shift in attacker behavior towards cloud-based services for email and online payment card processing typically using stolen credentials.
- Publishing errors in the cloud are increasing year-over-year, exposing at least 60 million records analyzed in the DBIR dataset. 21% errors due to misconfiguration and aligned to Sys Admin main threat vector.
- One quarter of all breaches are still associated with espionage.
- Media-hyped crypto-mining attacks were hardly existent
- The evolving job of the CISO/CSO is to understand how this large-scale digital relocation changes the landscape, and how they can manage the risk whilst embracing the opportunity.

DBIR is based on analysis of real world incidents and confirmed data breaches. Information is supplied by 66 external contributors to our VERIS framework

# Cyber Risk Understood?

It's a risk based world  
and organizations are insufficiently  
prepared for cyber threats

There is more talk about tech governance than action



Cybersecurity policies and defenses are the #1 corporate governance technology challenge, **yet only 21% of organizational leaders are briefed on risk topics at every senior leadership meeting**



53% of organizations believe that malicious attacks are on the rise y/y, but **48% don't feel confident in their teams' ability to address complex attacks**

# 87%\*

of board directors and C-level execs say they **lack confidence** in their organization's level of cybersecurity

Organizations need help framing the business case, prioritizing resources and spend to **improve cyber readiness and a way to benchmark progress**

\*

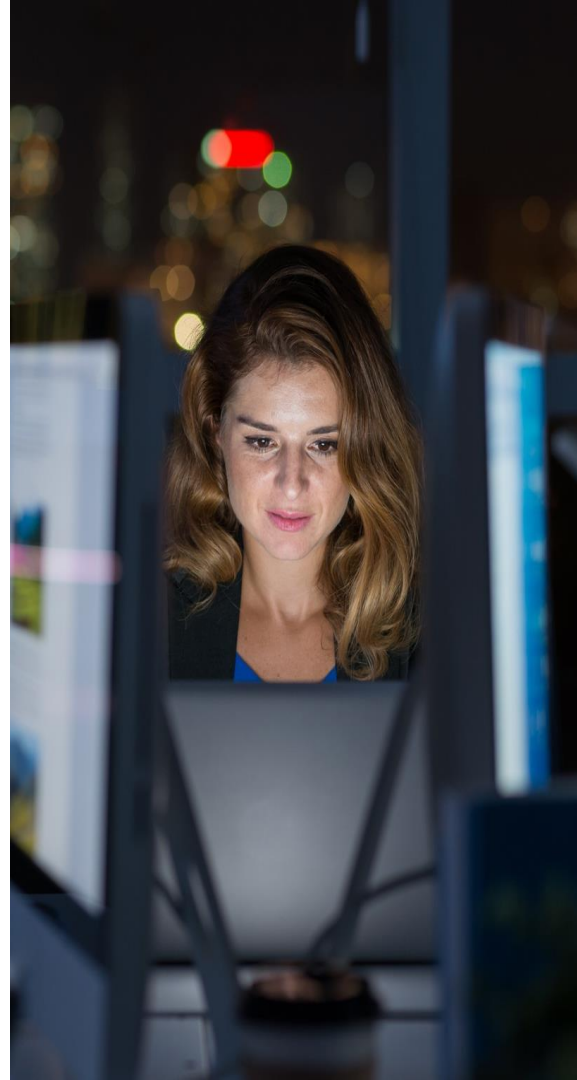
© 2017 ISACA. All Rights Reserved. Data Sources;

ISACA State of Cyber Security Report 2017 E&Y Report

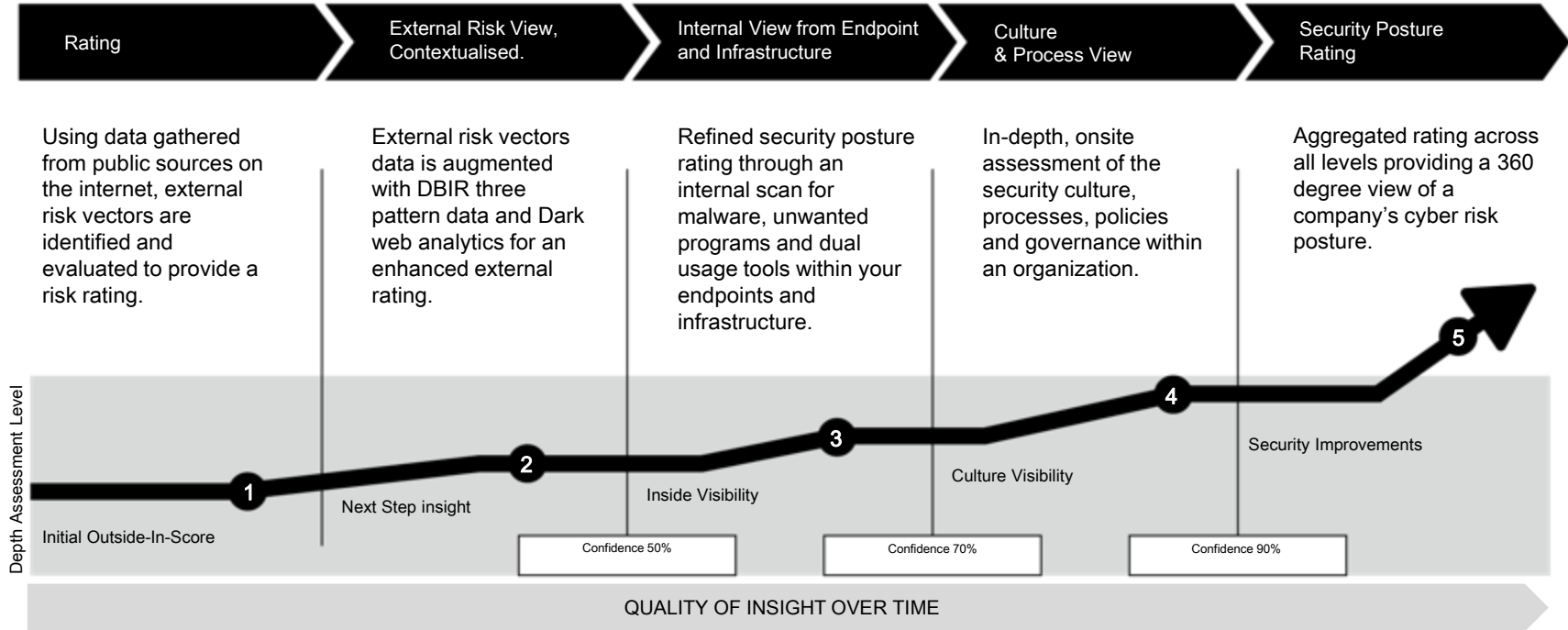
---

# 360° Risk Visibility

- In 63% of attacks where we know the motive for the attack there is a secondary victim.
- Traditional Risk evaluation is often done through point in time engagements
- Supply chain audit is increasingly burdensome, diverse in method and costly.
- Security programs must be programs of continuous improvement and their budgets and efficacy validated.
- Risk evaluation in M & A activity is increasing factor and workload.
- Strategic, Operational and Tactical information needs to be decoupled and provided to the right business user.
- Organisations and Service Providers need a dynamic tool to measure the efficacy of their security strategy.



# Quantifying security posture is key to mitigating risk.



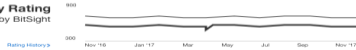
# Risk Report Sample



VRR My Infrastructure Notifications User Account

## VERIZON RISK REPORT

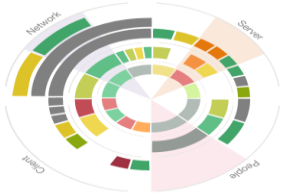
### Security Rating powered by Bitsight



**450** Risk Posture  
680

**C** Threat Level **4**

### Risk Compass



■ Denial of Service ■ Web App Attacks ■ Payment Card Skimmers

Industry: Finance  
Company Size: 500-1000 employees  
Geolocation: United States **Highlight industry risks**

### Prioritized Vectors

- Botnet Infections** Priority: **HIGH** Grade: **B** [View details](#)  
81% slower than industry for average duration.
- Web Application Assessment** Priority: **HIGH** Grade: **D** [View details](#)  
Web App Attacks are a major threat pattern in the finance industry.
- Systems in Poor Health** Priority: **HIGH** Grade: **C** [View details](#)  
Drop in score from 'A' to 'C' needs to be checked and remediated.
- Patching Cadence** Priority: **MED** Grade: **B** [View details](#)  
Emerging vulnerabilities have a high threat level.
- Endpoint Malware** Priority: **MED** Grade: **F** [View details](#)  
'F' grade needs to be remediated urgently.

### Chart Your Course

- Botnet Infections - avg. duration  
Current: 3.1 days Target: 1.8 days
  - Systems in Poor Health - risk not required  
Current: 5% Target: 2%
- Update charts**

### Threat Landscape

#### Industry Summary : Finance

Year: 2016

DoS attacks were the most common incident type.

Confirmed data breaches were often associated with banking Trojans stealing and reusing customer passwords, along with ATM skimming operations.

#### Top 3 Patterns



No. of Incidents



No. of Breaches



Data Compromised



Threat Actors



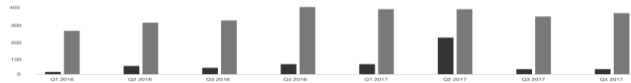
Actor Motives



Source: CSIR report

### Attention on Dark Web

Threat Level: **MEDIUM**



### Emerging Malware

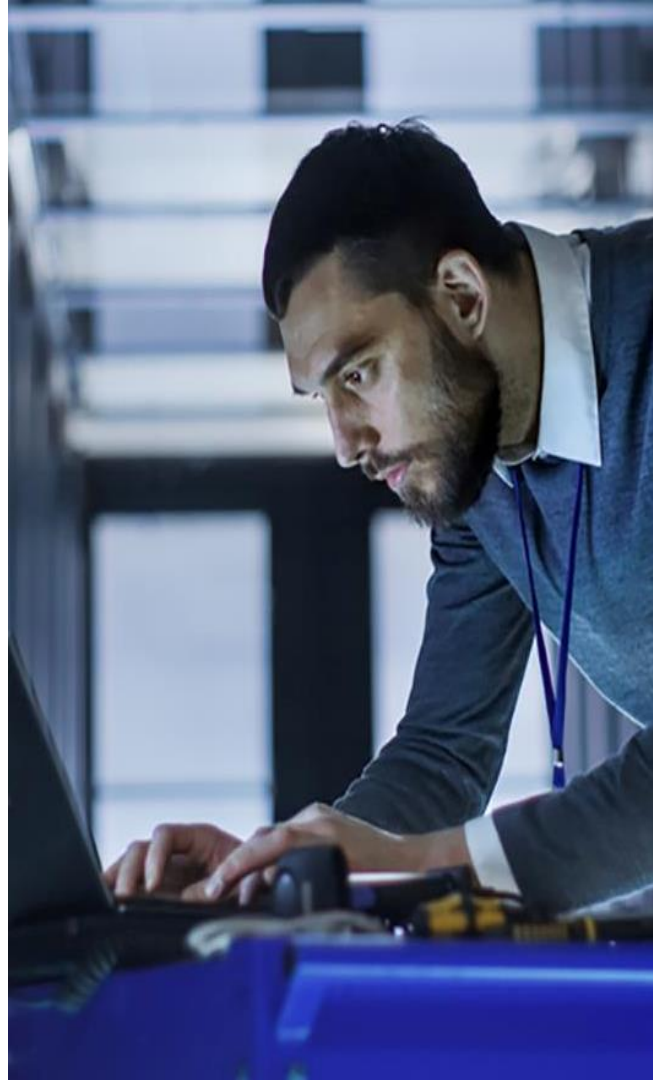
Threat Level: **MEDIUM**

- Kasidet**  
▲ Surge in cyber references in the last 60 days  
Affected Products:  
- Microsoft Windows XP  
- Microsoft Windows  
10 clients
- BackBot**
- GIBON Ransomware**
- Bad Rabbit**
- BrutalKangaroo**
- AKBuilder**
- Explo**
- Cherry Picker**
- Audiot**
- Blackdot**
- Others**

### Emerging Vulnerabilities

Threat Level: **MEDIUM**

- CVE-2016-10073**  
▲ Spike in cyber references in the last 60 days  
Risk Score: **Critical**  
Affected Products:  
- Microsoft Office 2007  
- Microsoft Office 2010  
- Microsoft Office 2013  
100 clients
- CVE-2017-0290**
- MS16-145**
- CVE-2015-2545**
- APSB15-14**
- CVE-2017-12611**
- CVE-2017-6331**
- CVE-2016-10045**
- MS05-011**
- Java Object Deserialize ...**
- Others**



# Thank You