Quantifying Risk Reduction: From War room to Board room.

Ali Neil

Director Security Solutions

10th October

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**

* Data Sources; ISACA State of Cyber Security Report 2017 E&Y Report

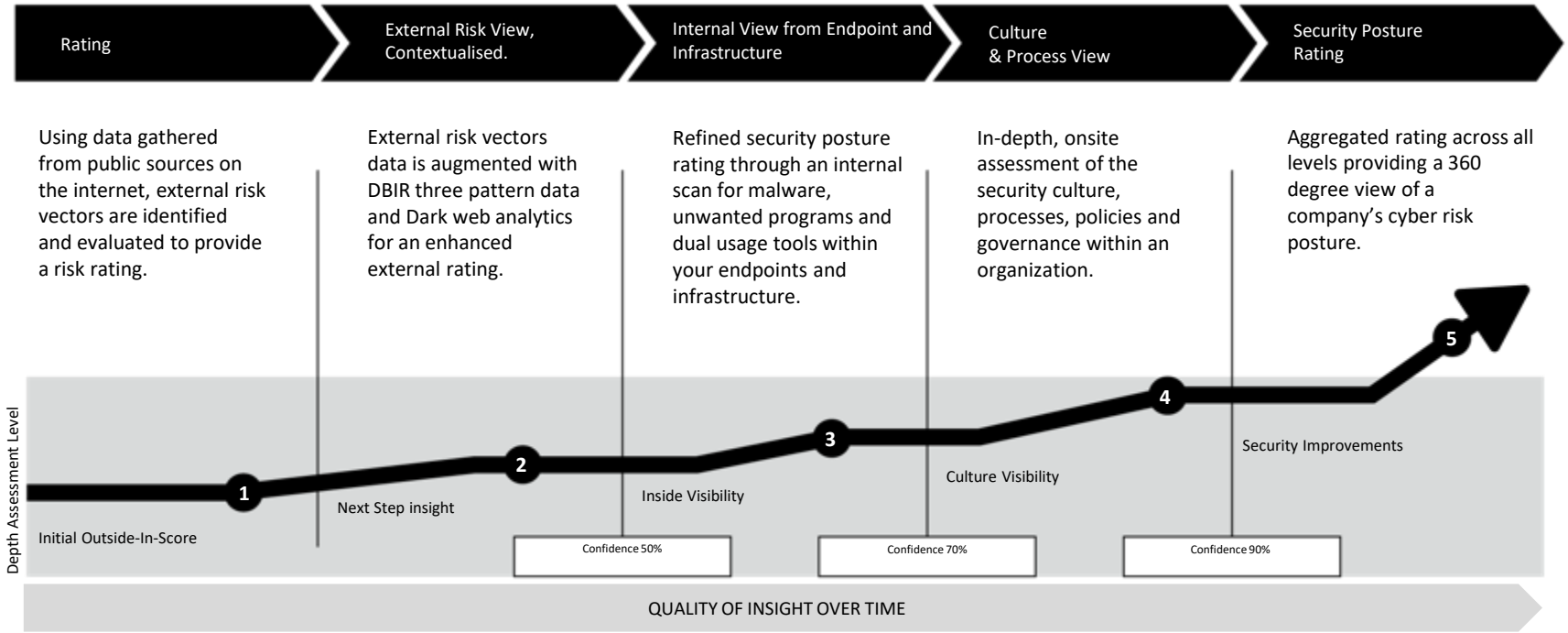
verizon

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.

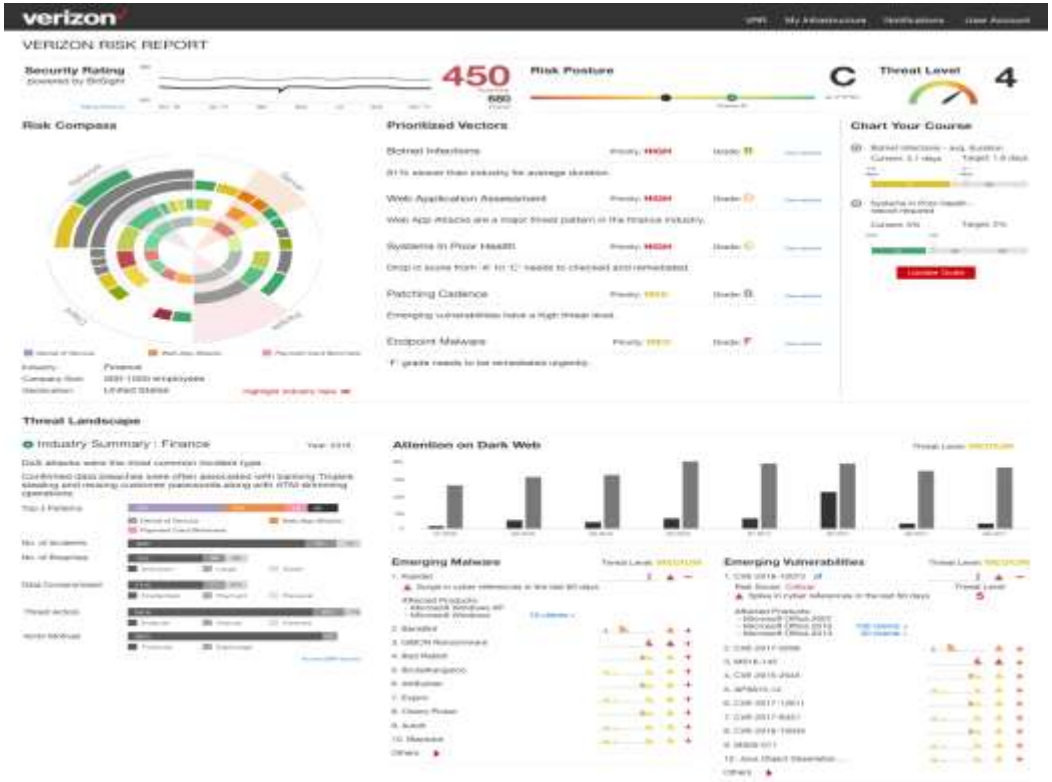
verizon

Quantifying security posture is key to mitigating risk.



verizon

Risk Report Sample

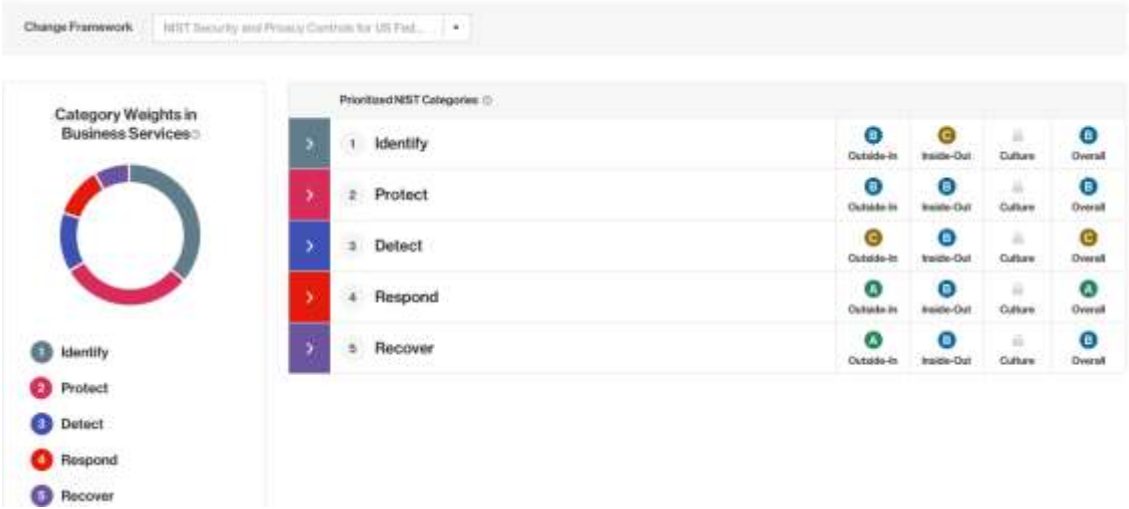


verizon

A framework of frameworks.

Security framework views

- DBIR threat patterns (Default)
- NIST cybersecurity framework v1.0
- NIST cybersecurity framework v1.1
- NISTIR 8183 manufacturing profile
- NIST 800-53 Rev 4
- NIST 800-53 Rev 5
- ISO 27799 PHI
- ISO/IEC 27018 PII cloud
- PCI-DSS version 3.2
- FFIEC cybersecurity maturity model



Thank You

verizon