Governance, Risk & Compliance: **New approaches to security metrics** OVERVIEW

Huntsman®
Defence-Grade Security Platform

The role of information security teams has evolved in recent years, and the historical context of protecting assets has established many trends and mind-sets. We are now seeing increasing interest from company directors in IT security, and trusted consultancy firms are advising this audience.

The last few years have seen big corporate cyber attacks and data breaches, interrupted operations caused by hacktivists and hefty fines for companies that exposed sensitive data. As a result, there has been a growing interest from boards in the way IT security functions operate.

Another factor is that technology transformation is no longer solely driven by projects, IT department or line management initiatives. The demand for new technologies is now coming from users: from board members who want to use tablet devices, and from increasingly mobile staff who are used to being connected to their business systems, clouds applications and social networks

QUESTIONS ARE MORE DIRECT

The effect of the growing interest from boards in IT security is that boards, internal audit committees and regulators are all expecting solid answers to very direct questions on information security. These tend to revolve around:

- The global and mobile nature of businesses, which means that the exposure from remote working is greater than just managing mobile devices;
- The challenge of keeping control of accesses, connections and data flows that occur more frequently on hosted cloud platforms outside of the organisation;
- An economic climate that has forced businesses to look more intently at costs and impacts, and to demand more value for money from technology and security investments.

The rate of change is speeding up rather than slowing down, and that is partly due to systems being more flexible (whether virtual or cloud-based) and to the increasing diversity of the end-user computing environment. This growth in power and flexibility has unlocked considerable innovation and led to a greater focus on data – both its protection and the value that can be derived from it.

48% of directors viewed data security as their top concern. 'These numbers have roughly doubled since 2008'.

Cybersecurity Risks and the Board of Directors, Harvard Law School, December 16, 2012

A NEW FOCUS ON GOVERNANCE, RISK AND COMPLIANCE (GRC)

There is clearly a growing need for the compliance status and risk position of systems, applications and platforms to be more carefully tracked and more readily visible. This reporting of security performance statistics or statuses, when carried out across a wider business environment, must consolidate information into a holistic picture of:

1. Compliance status;
2. Risk exposure;
3. Process operation and records.

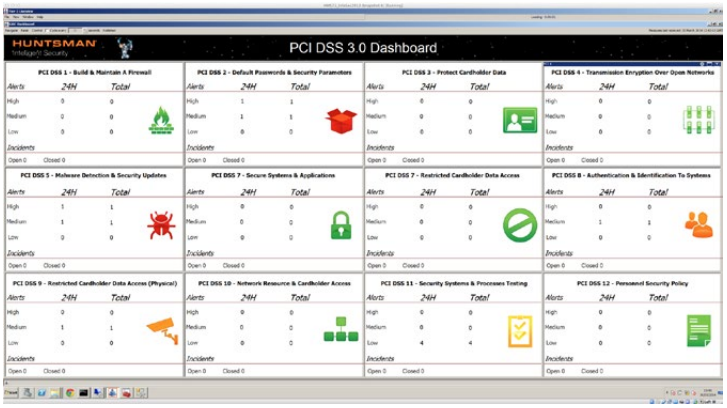
Boards and internal audit committees increasingly want to know about the effectiveness of processes, the balance between controls and risk acceptance, the financial implications of actions or inactions, and the potential harm caused by attacks.

Organisations that create service metrics around security often show glowing progress in patch and vulnerability management, present pie charts of user statuses and graphs that show steady and reassuring increases or decreases. However, these seldom provide the picture that is required. Businesses are affected by real-world events such as loss of revenue, financial fraud, compromise of valuable intellectual property, lack of competitiveness and reputational embarrassment. Typically, CEOs and directors worry about the impact on the business and its operations, not the technical failure that caused it.

A NEW VIEW OF THE WORLD

At Huntsman Security, we often provide both the data collection mechanisms and the reporting interfaces that security teams use. We have seen growing demand for more business-focused reporting, and we understand the need to present the outputs from security monitoring processes in clear terms that your board or audit committee will understand.

Organisations need to accept that the IT security view and the business perception of risk tend to be quite different. IT delivery functions tend to gravitate towards groupings based on location, network topology or technology types/families; the business tends to see end-to-end systems or processes.



Huntsman's GRC dashboard interface is a clear leap forward in business-oriented security and compliance reporting.

It uses risk information that is derived from the same source data sets, but the presentation is user-selectable so the dashboard will display what the IT team, the sales manager, the divisional director, the audit function and the CFO want to see within a view that is uniquely tailored to their needs.

CONCLUSION

Even the best IT security systems have seen failures. It follows that continuous monitoring, intelligent data analytics and clear visibility have never been more important. Compliance and security reporting is increasingly required to be both context-aware and tuned to a diverse audience.

Huntsman's IT security solutions have always employed analytics across a range of data sources, and embraced the concepts of big data, trend analysis and intelligence. Now we have added much clearer visualisation of business risk to respond to the needs of C-level managers and directors who want to pay closer attention to Information Governance.

Huntsman | Tier-3 Pty Ltd

Asia Pacific

t: +61 2 9419 3200
e: info@huntsmansecurity.com

Level 2, 11 Help Street
Chatswood NSW 2067

EMEA

t: +44 845 222 2010
e: ukinfo@huntsmansecurity.com

100 Pall Mall, St James
London SW1Y 5NQ

North Asia

t: +81 3 5809 3188
e: info@huntsmansecurity.com

TUC Bldg. 7F, 2-16-5 Iwamoto-cho,
Chiyoda-ku, Tokyo 101-0032

Americas

toll free: 1-415-655-6807
e: usinfo@huntsmansecurity.com

Suite 400, 71 Stevenson Street
San Francisco California 94105

huntsmansecurity.com

linkedin.com/company/tier-3-pty-ltd

twitter.com/Tier3huntsman