M&A Security Due Diligence Diagnostic©

TrustedImpact
PROTECTING DIGITAL

Have you bought an information security breach?

The Issue:

Experts from accounting, venture capital, consulting, and law firms can be very good at assessing the profitability and potential synergies of a merger or acquisition. Yet little, if any, attention is paid to the security posture of the organisation under scrutiny – often with disastrous results.

Why? The exponential growth of "Identity theft" and the significant ramifications of lost sensitive information has now become a significant board-level issue. In fact, for most enterprises today the unfettered availability of key information is now literally the lifeblood of the business – its loss, modification or disruption is disastrous. Also, global public disclosure laws are emerging, such that companies that have not applied a duty of care and who lose sensitive information can now realise significant losses in the form of personal liability, fines, class action law suits, tarnished reputation and lost customers.

By taking a complete look (including information security) at the relevant sources of value and risk, the chances of a successful acquisition increase significantly.

Information security:

Standard Merger and Acquisition (M&A) due diligence checklists rarely address information security topics across people, processes and technology. It is not adequate to request the seller for a representation that it uses "reasonable security measures" to protect sensitive information.

The objective of information security due diligence is not reject or rubber-stamp the transaction, but rather provide a more complete picture of the unique risks for decision makers.

Prevention strategy:

Assessing the information security posture of the target organisation benefits the acquiring company in numerous ways:

- Provides an objective third-party assessment using seasoned experts, rather than generalists
- Enables the acquirer to better determine an acquisition price for the risk it may be purchasing
- Provides resources and expertise usually not available internally
- Enables the communication bridge between IT, security and the Boardroom
- Frees critical internal resources to focus on keeping operations running smoothly

What's at risk?

Customer trust and retention
One of the most highly publicised emerging risks today, is the data security breach. Companies losing control of sensitive customer information today, face angry customers who take their business elsewhere.

Disgruntled ex-employees
As jobs are rationalised, former employees with detailed knowledge of internal systems may pose a threat.

Investor confidence
Avoid surprises and help realise the shareholder value that made the deal attractive in the first place.

Security-related regulatory, legal and compliance

Integration challenges

Legacy burdens
People, process and technology

IMPACT OFFERING

Identity theft - one of the fastest growing crimes in the world

In only those locations that legislate public disclosure, **290 million** personally identifying records have been lost in the last 3 years

31% of customers terminate their relationship with organisations following a data breach

9% (or ~2 Million) of Australians have been victims of Identity Theft

81% of companies failed to perform the basics of information security (lacked basic software patches, disabled firewalls, and did not update security software)

M&A Security Due Diligence Diagnostic©

TrustedImpact
PROTECTING DIGITAL

IMPACT OFFERING

Demonstrates the Board has applied their 'duty of care'

Ensures a deal valuation better reflects the true risk of the target

Faster, better – security professionals assessing your security posture, not auditors ticking checklists

Provides a clear 'baseline' for potential consolidation, rationalisation and integration savings

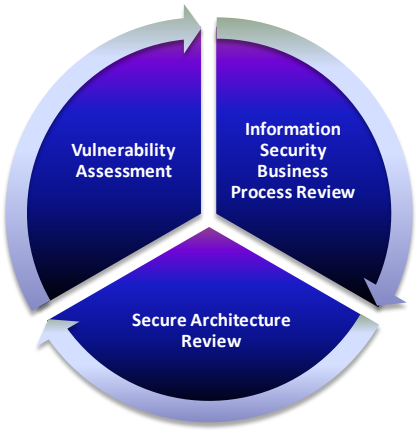
Business landscape holistic – Recognises that 33 percent of breached records are from trusted 3rd party partners

Further information:
Trusted Impact Pty Ltd
Level 9, 22 Albert Road
South Melbourne, VIC 3205
Australia
(03) 9023 9710
info@trustedimpact.com.au
www.trustedimpact.com.au

The Approach:

We approach the problem from three (3) dimensions, which provide different perspectives, which are all aimed at uncovering key risk areas. This approach involves:

Use of automated tools to detect vulnerabilities on critical ICT assets



People/Process review across key security domains to determine the maturity of information security

Technical review to identify significant weaknesses or exposures in the ICT environment

The Offer:

Our M&A due diligence diagnostic will provide you with an assessment of your high risk security areas, and practical steps to improve the protection of your critical business information at a fraction of the time and cost. We apply a comprehensive framework of evaluation (illustrated below), and **within 3 to 6 WEEKS**, can help you understand where key risk areas reside:

Technology:
- System access / control
- Internet and e-mail usage
- Remote access
- Mobile computing
- Use of personal devices
- Network controls
- Intrusion detection systems
- Firewall – Antivirus – Malware
- Software licences
- Software development
- Data backup
- Audit logging

Physical:
- Defense-in-depth
- Operational facilities
- Headquarters
- Remote sites
- Storage

Organisation:
- Roles & responsibilities
- Ownership
- Compliance & documentation
- Incident reporting

Policy:
- Strategy & Applicability
- Education and awareness
- Roles and responsibilities
- Monitoring and Review
- Penalties for breach
- Code of Conduct
- Business Continuity

Business Systems:
- Risk identification
- Control identification
- Incident management
- Key Points / Vulnerable Points
- Accounting systems
- Management systems
- Disaster Recovery

Third Parties:
- Regulators
- Outsourcers
- Contractors
- Strategic alliances
- Govt. – State & Federal

People:
- Risk identification
- Control identification
- Incident management
- Fraud, compliance, & control

Data:
- Classification – sensitive or critical
- Protection of data, IP and clients
- Handling and Storage
- Privacy
- Security of IT platform(s)
- Archive and retrieval

Processes:
- Segregation of duties
- Control of access
- Computer Room
- Control rooms
- Intruder detection & alarms
- Security of business procedures
- Employment Contracts / Confidentiality agreements
- Contractors & third parties
- Asset management

Our professionals are highly qualified and experienced information security professionals who understand the complexities facing most enterprises and can quickly assist you to understand your target's security position.

In the age of information and information technology, no due diligence is complete without knowing the security of the target company's information. Don't buy an information security breach. Do your due diligence and let the experts at Trusted**Impact** help you.

... for further information call Trusted**Impact** on (03) 9023 9710.