Ensuring Cyber Security Due Diligence during an Acquisition

Abstract

Since the focus of a merger or acquisition, or spin off is usually on enhancing competitiveness or scale of operations, cyber security is typically put on the backburner. The cursory due diligence conducted before an acquisition seldom results in a robust security posture. The immediate challenge for a chief information security officer (CISO) after a merger, is ensuring that the new entity has a security baseline that measures up to the risks it faces.

The CISO usually seeks to answer questions such as:

- How can we ensure that the acquired company matches the current cyber security posture?
- Which security functions and components do we need to upgrade?
- How can we ensure at least minimum baseline security?

We recommend a framework that presents a holistic view of security functions, controls, and activities that an organization could undertake to address the questions posed above. With this framework, CISOs can identify and mitigate structural shortcomings in the cyber security posture of an acquired or spun-off entity.

Ensuring a robust security posture during M&As

Despite the global M&A volume of $3.9 trillion in 2016,[1] organizations are only now waking up to the importance of the cyber security posture in an M&A transaction. We suggest a framework (seen in Figure 1) that can help CISOs answer the questions they may have on cyber security as well as strengthen the present security posture by supplementing it with additional controls in the event of an M&A or a spin off. Enterprises and conglomerates that consist of multiple business entities can use it to arrive at a common minimum baseline to ensure a consistent cyber security posture across all entities. CISOs of new entities formed from a spin off may also find the framework useful in constructing or firming up its security posture. The framework is easy to use and is based on the five high-level functions defined in the NIST Cybersecurity Framework. Each component can be customized based on the industry and business, applicable laws, regulations and standards, risk appetite, and security budget.

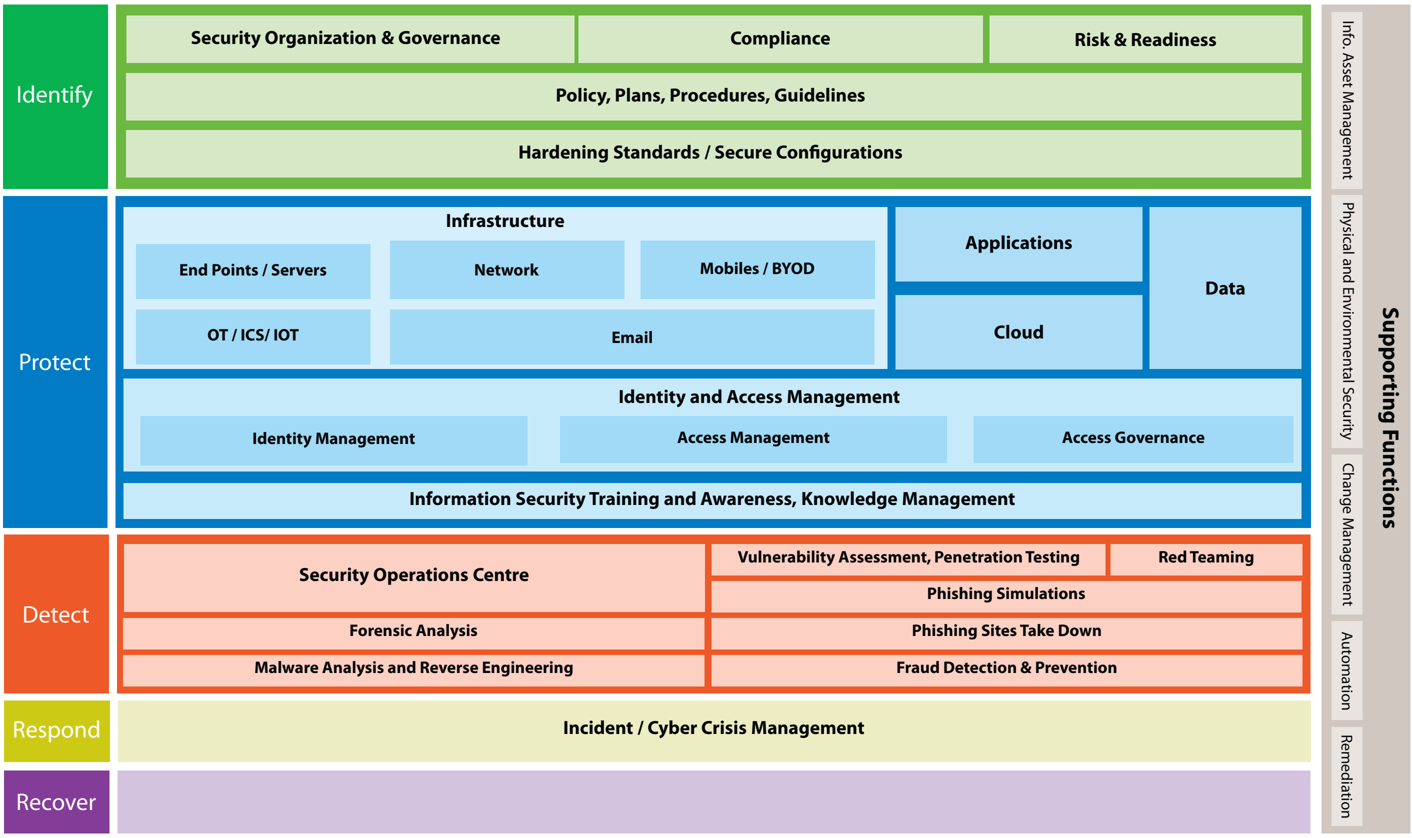
Identify
Security Organization & Governance
Compliance
Risk & Readiness
Policy, Plans, Procedures, Guidelines
Hardening Standards / Secure Configurations
Protect
Infrastructure
End Points / Servers
Network
Mobiles / BYOD
OT / ICS/ IOT
Email
Applications
Cloud
Data
Identity and Access Management
Identity Management
Access Management
Access Governance
Information Security Training and Awareness, Knowledge Management
Detect
Security Operations Centre
Vulnerability Assessment, Penetration Testing
Red Teaming
Phishing Simulations
Forensic Analysis
Phishing Sites Take Down
Malware Analysis and Reverse Engineering
Fraud Detection & Prevention
Respond
Incident / Cyber Crisis Management
Recover
Supporting Functions
Info. Asset Management
Physical and Environmental Security
Change Management
Automation
Remediation

Figure 1: An overview of the recommended cyber security framework

A framework for due diligence

#1 Identify

This is the first step that the information security team should take in the event of a merger. This would involve identification of different aspects of the security posture such as:

- The existing security organization and its governance structure, including people – the identified tenets include staffing, reporting, escalation paths, and security metrics.
- The regulations, laws, and standards to be followed along with compliance mandates.
- Security risks such as cyber supply chain risks, third party risks, and the organization's readiness to face eventualities such as a forensic investigation following an incident.
- Security controls governing the IT operations and practices that need formal documentation in the form of policies.
- Practices such as bring your own device (BYOD) and cyber crisis management along with the information security policy and privacy policy.
- System hardening standards and secure configurations based on the technology stack. To draft these standards, organizations can use OEM guidelines and industry best practices along with guidelines from credible bodies.

#2 Protect

This function defines the defensive side of an organization's cyber security posture and could include infrastructure, applications, data, identity and access management, and knowledge management.

Infrastructure

This addresses security at end-points and servers. Infrastructure network security covers conventional solutions such as firewall, data loss prevention (DLP), and network intrusion detection and prevention systems (NIDS and NIPS). And should also include more solutions such as advanced persistent threat (APT) defense and distributed denial of service (DDOS) protection. It is ideally based on the types of risks an organization faces and the business impact of those risks. If mobiles device are allowed under BYOD, they should also be included. CISOs could also consider baselining, policy enforcement, mobile device management solutions, and encryption.

Email too can be protected with solutions such as DLP, anti-spam solutions, and encryption. With regard to cloud migration, since security governance is at a nascent stage, a sound cloud protection strategy is required. For the cloud, priorities include cloud access security broker (CASB) and agreeing upon SLAs and contractual clauses with the provider, and solutions that address infrastructure, application, data, and network security. Operational technology devices (OT) can be protected using measures such as hardening, patching, and application whitelisting. The guidelines from the US Department of Homeland Security suggest measures to address the security concerns around IoT infrastructure.[2]

Applications

Application security measures include secure design, threat modelling, secure coding, code reviews, vulnerability assessments, penetration testing, as well as the implementation of a web application firewall.

Data

Data security measures need to be carefully built based on what data needs to be protected. Apart from security solutions, security processes are an inherent part of the data protection strategy. These processes include data classification, data discovery, non-disclosure agreements for contractors and vendors, data retention, and destruction. Conventional solutions such as electronic documents management (EDM), electronic records management (ERM), as well as database activity monitoring (DAM), data masking, hashing, and encryption solutions can also be deployed as part of these processes.

Identity and access management

Managing, controlling, and governing identities and related access tools are the foundation of a sound cyber security protection strategy. Business needs might mandate solutions for privileged access, access governance, identity lifecycle management, or password management.

Knowledge management

People are often the weakest link in a cyber security strategy making the knowledge management sub-function an indispensable part in the framework. In addition to training and awareness, knowledge management ensures that employees have the needed security knowledge.

#3 Detect

A robust and agile detection function is important for cyber resilience. This function addresses the security operations center, vulnerability assessment, digital forensics and malware analysis, and phishing simulations and fraud detection.

A modern security operations center (SOC) establishes effective detection rules. It monitors security information and event management (SIEM) output as well as manages the threat intelligence eco-system, user behavior and security analytics, and even intrusion prevention and detection systems (IDS and IPS) for swift action. The vulnerability assessment (VA), penetration testing (PT), and red teaming exercises are often very potent means to gauge the effectiveness of security controls. Regular VA and PT exercises, supplemented with red teaming ensure effective detection. Digital forensics and malware analysis help organizations act swiftly to contain damage from a breach, support legal redressal, as well help estimate the extent of the breach. Finally, this function involves removal of phishing sites and holding phishing simulation drills to detect employees who are susceptible to phishing attacks. It also includes deploying fraud detection and prevention solutions based on the risk appetite of the organization.

#4 Respond

Consider how to use people, processes, and technology to manage a response to a breach. It defines the roles and responsibilities of executives who undertake particular activities during an incident. Define processes such as procedures to be followed to manage an incident and the communication matrix to be followed for different stakeholders. Deploy an incident lifecycle management tool as well as capabilities to preserve and produce evidence, and run e-Discovery in the case of a litigation.

#5 Recover

Preparation is fundamental to the recovery function. Here, a business continuity and disaster recovery (DR) framework and policies and procedures are required. These can be supplemented with DR drills and maintenance of backup data, baseline images, and last known good configurations as well as cyber insurance.

Support functions: Liaising and coordinating with other operations

Certain aspects of IT operations do not fall under the ambit of the CISO's responsibilities but have a bearing on security operations. To ensure security objectives and SLAs are met, liaison and coordination is required with these support functions. These could include functions such as information asset management, change management, automation, physical and environmental security, and remediation.

Together this framework enables CISOs to construct or structure a cyber-security posture quickly in a modular fashion.

Growing importance of cyber security postures during M&As

Boards of directors are beginning to pay greater attention to an M&A target's cyber security posture during due diligence. The New York Stock Exchange and Veracode conducted a survey among directors and executives to determine the importance of cyber security in M&A due diligence processes. More than half of surveyed directors and officers claim a high-profile breach would significantly lower the valuation and one out of five say the revelation of a high-profile data breach at an acquisition target would deter them entirely from proceeding with the deal.[3] A holistic view of security functions, controls, and activities that an organization should undertake, can enable CISOs to successfully ensure security in an M&A or spin off..

References

[1] JP Morgan, 2017 Global M&A Outlook, January 2017, accessed July 2017, https://www.jpmorgan.com/jpmpdf/1320723701797.pdf

[2] Department of Homeland Security, Seven Steps to Effectively Defend Industrial Control Systems, December 2015, accessed July 2017, https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

[3] NYSE, Cybersecurity and M&A Due Diligence Process, 2016, accessed July 2017, https://www.nyse.com/publicdocs/Cybersecurity_and_the_M_and_A_Due_Diligence_Process.pdf

About The Author

Vivek Kaushik

Vivek Kaushik is part of the Fraud Management and Digital Forensics Center of Excellence (CoE) with TCS' Cyber Security Practice. Vivek has a diverse experience of more than eight years in vulnerability management, penetration testing, privacy and compliance, fraud management, and digital forensics. Vivek is currently leading sales for fraud management and digital forensics services. He holds a Bachelor's degree in Technology, Master's in Business Administration, and a Post Graduate Diploma in Cyber Law and Cyber Forensics.

Contact

Visit the TCS' Cyber Security page on www.tcs.com

Email: cyber.security@tcs.com

Subscribe to TCS White Papers

TCS.com RSS: http://www.tcs.com/rss_feeds/Pages/feed.aspx?f=w
Feedburner: http://feeds2.feedburner.com/tcswhitepapers

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model^{TM}, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

Experience certainty.

IT Services
Business Solutions
Consulting

TCS Design Services I M I 11 I 17