Radiflow

Mergers, Acquisitions and Divestitures – Thinking about Cybersecurity?

November 2022

Introduction

The 2021 Fortune 500 CEO survey documents that two-third of the interviewed CEOs consider cybersecurity risk as their greatest concern. The implications of this rising source of risk are significant in the context of mergers and acquisitions (M&A), as M&A transactions offer sophisticated cyber terrorists an opportunity to target the firms involved. The process of data migration and integration conducted in the immediate aftermath of the acquisition is complex, sensitive and exposes high-value data to potential cyberattacks, which is often further compounded by media coverage attracting the attention of bad actors.

The industry has witnessed where the lack of good cybersecurity has a direct impact on M&A deals. In 2016, TalkTalk, a U.K.-based telecom business, was fined £400,000 when a threat actor accessed a customer database it acquired earlier was hacked. In 2017, the price of Verizon's acquisition of Yahoo's internet business plunged $350 million after Yahoo disclosed three massive data breaches compromising more than one billion customer accounts. And, companies exploring M&A today would be wise to consider a recent example from April 2020. A pending merger had 5% of its total purchase price set aside to cover the potential fallout from a ransomware attack. (Source: SecurityIntellignce)

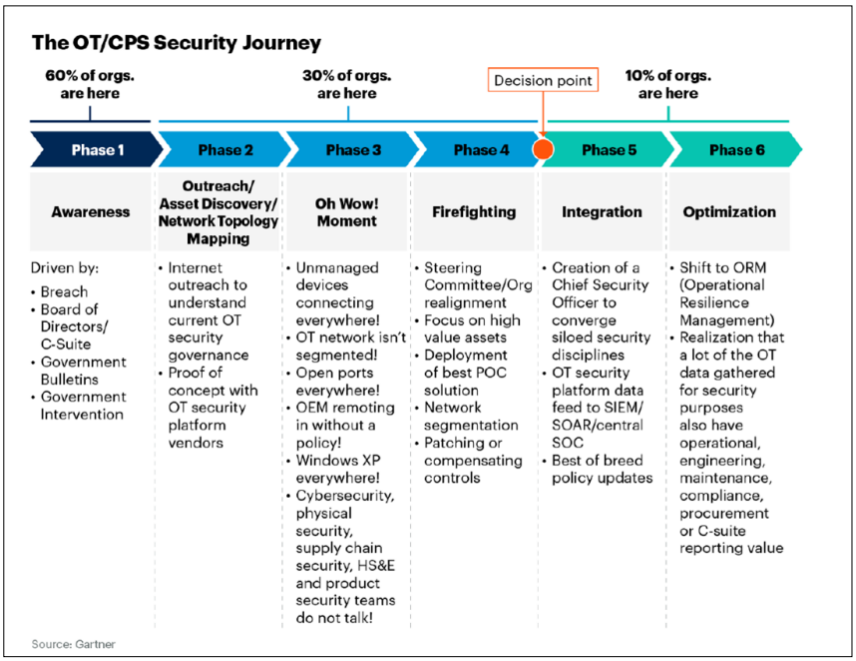
As such, knowing what you are buying from a cybersecurity perspective, along with sustaining a good cybersecurity posture in your own business is becoming more critical from the deal price as well as understanding what level of historical risk you are buying or even selling.

Why is it important to focus on OT as well as enterprise security during M&A?

In the OT Cybersecurity journey, Gartner information shows that 60% of companies are at the beginning in awareness and only a small proportion are actively managing a program to start the firefighting. This coupled with OT environments historically being less connected to either internal or external networks has created almost a sheltered ecosystem where the "OT engineer" typically has accountability for both machine and embedded technology. Their focus is on safety, quality, OEE, maintaining an asset with a long life cycle (20yrs+) and typically less on security hygiene.

The concept of traditional IT practise in cybersecurity, like patching, network design etc has only recently become a factor that needs to be embedded into OT, driven by the emergence of digital, the drive to connect the OT environment and increased malicious acts and malware.

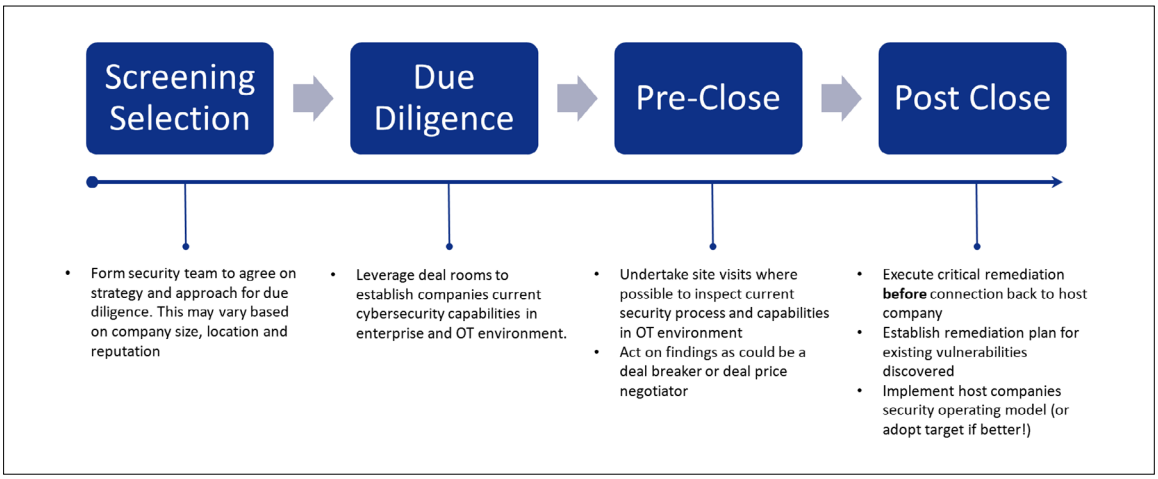
Today, the OT environment is catching up on cybersecurity safety whilst holding key critical company IP in both R&D and Manufacturing and some fairly open exposure for malicious actors to leverage. As such, being able to see what assets a company has, how they are connected, their vulnerabilities and potential impact to critical systems, is a real priority.



Applying Cybersecurity Diligence in the M&A Process

The diagram below shows a typical flow during and M&A approach. It's not unusual for companies to ask questions about security posture of the target company, albeit many companies may leave this too late in the M&A process. Capture can happen during the deal room process in the early phases, or may be executed later with site visits and questionaries' to establish current process and practise before the deal is closed. At enterprise IT level, it's usually less complex to establish where a target company stands, however when exploring OT, many challenge may arise. These range from:

- Not knowing what the target company has and the sheer volume of OT assets
- Many undisclosed third party links and potential contract manufacturers connections
- Access to the right people that know OT; typically "IT" are involved but not so much the OT engineers
- Potentially sensitive areas to gain access to
- A plethora of legacy and ageing systems



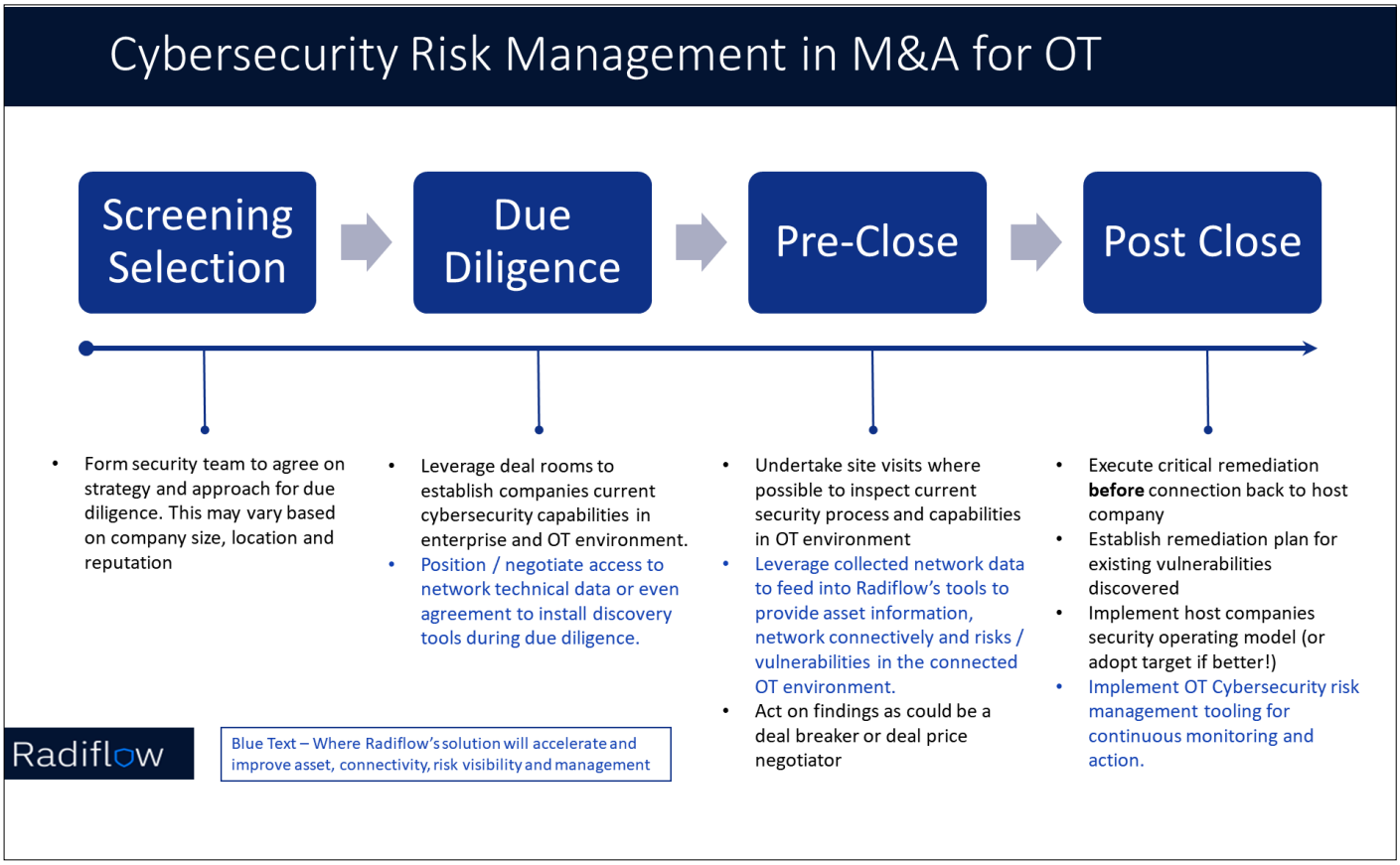
Leveraging Radiflow's tooling during and after M&A to reduce risk and sustain good security posture

Building on the earlier diagram and process flow, below shows where Radiflow solution can be added to accelerate understanding and reduce risk in both acquiring a company, or within a merger or divestiture situation to share the current risk posture of the company being sold or merged.

Leveraging this type of tool provides benefits in risk management, understanding the vendor estate of platforms being acquired, helping plan the integration / costs and providing visibility to the supply chain to understand connected vendors.

The challenge in an acquisition space will be down to the level of "access" that can be gained to a targets facilities and networks. The ideal would be to deploy tooling that can non-intrusively detect and collect asset information and build into a network view showing "current" risk and vulnerability posture.

Where technology cannot be installed at the target location an alternative approach would be to leverage the target companies PCAP network files and feed those into an instance of CIARA. CIARA will then provide a read out of current topology and risk posture.



Conclusion

As the world starts to realise that buying or selling a company with inherent cybersecurity risk can have near term significant cost and impact through targeted attack (data theft or malicious) or longer term impact via fines levered for past performance, early understanding of the Cybersecurity risk posture in an M&A transaction can play a significant part in the deal price and future investment value realisation.

The process of due diligence must be extended to take a hard look at current and historical cybersecurity posture and factor this into the deal price and potential risk appetite.

Today in M&A it is not unusual to go on site and inspect what you are buying, so why not go a stage further, and if you like, undertake a building survey to see what the technology is telling you? Leveraging tooling, where permitted to undertake a discovery and risk assessment will enable a much clearer view as to security risks, current assets and connectivity.

An interesting further read from Deloitte can be found here.

Radiflow Products overview and how they can help

Leveraging technology for discovery and risk management of OT connected systems and devices can both accelerate an organisations understanding of their risk posture and provide ongoing and near real time visibility to a changing internal and external threat landscape.

Radiflow's products bring industry excellence in the discovery and risk management of OT at enterprise level with additional industry leading value from enterprise risk visibility, laser focused reporting and planning by critical assets. These products enable a CISO to quantify and prioritise risk and impact in ways that business owners will understand and jointly support funding proposals.

Radiflow's OT-security suite has been successfully implemented in a number of major organisations worldwide.

Radiflow's multi-prong solution provides anomaly detection and threat monitoring within an OT environment (manufacturing, utilities, transportation, power etc) to ensure the detection of breach attempts originating from the IT network. The Radiflow solution further improves network oversight by providing full visibility (via network "maps") into the OT network, including all and device properties, vulnerabilities, communication protocols and possible intra-network attack vectors.

The Radiflow Workflow

Once discovered, assets are grouped into Zones (connected by Conduits) to facilitate IEC 62443-compliant risk assessment & management.

Using multiple data feeds for newly-discovered threats and vulnerabilities, as well as rich contextual information received from equipment vendors for cybersecurity analysis, Radiflow's threat detection and monitoring solution provides operators full control over anomaly alerting and incident handling.

Going beyond threat detection, network visibility and security assessment, Radiflow's risk management platform empowers users to optimize their cybersecurity expenditure by prioritizing the threats that pose the most risk to the organization as a whole (accounting for the impact of a debilitating attack on each zone/business unit or critical asset) and subsequently the mitigation measures best suited to reducing the most risk and thus increasing the ROI of the entire cybersecurity operation.

Radiflow's risk assessment process involves analysing thousands of network data points and asset properties, threat intelligence and impact calculation to provide various KPIs and full reports for the network's risk state:

- Network and asset properties: using non-intrusive self-learning of the OT network, Radiflow creates a complete digital image of the network with all network, communications and assets properties and vulnerabilities. The digital image serves as the baseline activity model for assessing risk and OT cybersecurity planning.
- Threat intelligence: newly-detected threats and threat players' capabilities are analysed and published by a number of dedicated agencies (e.g. MITRE ATT&CK) as well as by others, including Radiflow's own research.
- Zone impact & criticality, risk tolerance and other considerations: assets and business processes are grouped into zones with different levels of criticality and security needs.

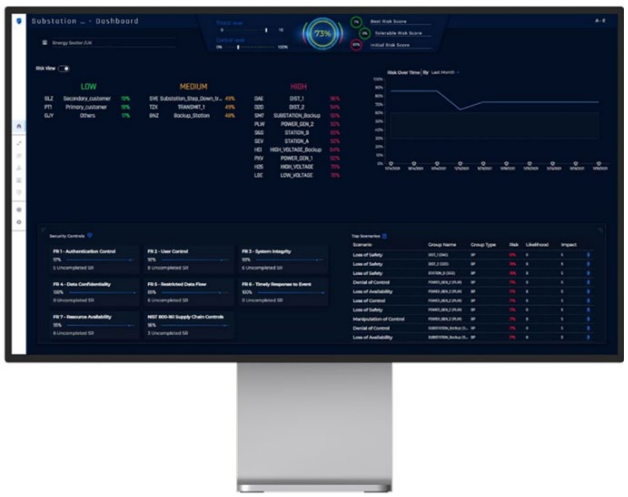
The CIARA Risk Assessment & Management Solution

Radiflow's CIARA OT Risk Assessment & Management Platform analysing thousands of data points for network and asset properties, threat intelligence and impact calculation, toward providing various KPIs and full reports for the network's risk state.

All asset, network, threat and SuC owner-provided data points are used to run numerous non-intrusive breach and attack simulations

The simulations determine the most impactful threats to the network and subsequently the most effective mitigation controls that deliver the most risk reduction per dollar spent.

The results of Radiflow's risk assessment are provided in the form of various high-level and detailed reports used for budgeting, auditing and follow up, as well as a detailed mitigation plan listing the most effective (high-ROI) mitigation measures, accounting for the user's budget and risk management preferences.



By running numerous breach & attack simulations (BAS) based on multiple sources for threat intelligence, device vulnerabilities, network attributes and more, CIARA is able to provide decision makers with KPIs for overall risk, threat level and control level (completion of mitigation meausres) as well as a comprehensive mitigation roadmap that prioritizes mitigations that deliver the most overall risk reduction. The result is optimized, high-ROI OT security system.

About Radiflow

Radiflow develops unique OT cybersecurity tools to protect and ensure organizations' digital resilience. The company closely collaborates with Managed Security Service Providers to oversee the discovery and management of all relevant data security points. Founded in 2009, Radiflow has offices and partners in Europe, USA and APAC. Its field-proven solutions are installed at over 7000 sites around the globe.