NTT Security

Whitepaper

Going After the Weak Link

Security in Mergers & Acquisitions

Information security is a key element of successful Merger and Acquisition (M&A) projects.

The importance of Governance, Risk and Compliance (GRC) should be kept in mind throughout the processes of due diligence, closing the deal, and "Day One" activities that begin the integration of acquired companies.

Attackers know that a company is only as strong as its weakest link. When seeking access to valuable company data, such as intellectual property, credit card data or health information, attackers will try to infiltrate email, network shared drives, and other resources. In order to control a company's core IT services, they often find that an indirect route is the most successful.

A large global company typically will have established policies and strong cybersecurity defences at its corporate headquarters, but it is not uncommon to find that security is lax at some of the company's acquired divisions.

- An attacker will look for acquisitions and subsidiaries in order to find insecure perimeters, such as firewalls that allow Telnet or Remote Desktop access directly to the internal network.
- Once inside the acquired company's network, the attacker then seeks connectors into the central corporation through Active Directory federation or connectivity put in place for databases and applications.
- If the attacker finds a link, that opening is used to gain a foothold inside the well-secured corporate network.

It is not difficult for attackers to locate the weak links. Many acquisitions are publicly announced in press releases and noted in industry journals and news feeds. Additionally, public companies include the list of their subsidiaries in SEC filings, which can be searched online at www.sec.gov. Most organizations also release Annual Reports online, with merger and acquisition information included to demonstrate the company's strategy for growth.

Weak Branches can bring down a Strong Tree

It is initially difficult to understand why a company would not put forward the effort to secure its acquired divisions. **However, this is often a management decision based on business priorities**.

For example, consider an international manufacturer (we will call Acme) that has purchased a small start-up. The start-up, which has developed a unique technology, consists of just eleven people – ten engineers and one office manager.

When Acme first bought this start-up (which we'll call Genius), a key engineer threatened to walk off his job if he was restrained in any way by new policies and procedures. The executives at Acme assured him that there would be no changes, no red tape, nothing to interfere with the creativity of Genius. Moreover, the CIO at Acme was told to make sure that the employees of Genius had all the resources they needed and none of those bothersome rules; rules like separation of duties, encrypted data transfers and multi-factor authentication.

It was assumed that over time the employees at Genius would adapt to Acme's company culture and adopt the policies and procedures in use there. That did not happen. In fact, the engineers at this branch location took pride in being able to work around the security restrictions that the parent company tried (at times) to impose. When corporate security put a firewall between the development lab and the production network, the chief engineer walked into

the wiring closet and unplugged the firewall. "Honey badger don't care," he said, by way of explanation.

The engineering team found ways around corporate requirements, installing rogue access points, routers and switches. When internal audit performed a site visit, these problems were reported back to corporate headquarters, but were given low priority because they were found on an "acquisition network."

Eventually, an attacker discovered this small division of Acme where all the users were domain administrators and developers had access to production systems; where there was no network segmentation between development, test and production. Moreover, it was simple to infiltrate the network, because numerous avenues had been left open for engineers who work from home or on the road. VNC, without encryption, was the remote access protocol in use.

- Once inside, the hackers found the golden key – the small shop's Active Directory was integrated into the main corporate Active Directory.
- They gained access to the corporate Active Directory, email and network shared drives, using a compromised administrative account.

How long did the hackers work inside the network, perusing Acme's email and data? No one knows for certain; one evening the CEO noticed some oddities in his email and called the CISO: "I think I've been hacked."

Start at the Start – Due Diligence

One of the best ways to integrate information security into Mergers & Acquisitions is to include information security and compliance in the due diligence process. When conducting due diligence, the acquiring company reviews a large amount of documentation from the "target" – the company it may buy.

- The acquirer should ask for all information security and privacy policies and procedures, security training programs, vulnerability scan and pen test results, network maps and other relevant administrative and technical documents.
- These should be inspected to determine the level of security governance at the target and identify gaps in policy and operations.

Specifically, the security program at the target company should be reviewed in light of the existing security framework used by the acquiring (parent) company. The parent company may comply with PCI DSS, HIPAA or other regulations. It may have developed security policies in line with NIST Cyber Security Framework, ISO/IEC 27001 or NIST SP800-53. How does the security at the target company compare? What are the gaps? This gap analysis will provide a baseline to understand how the acquired company differs from the main corporation.

Consider as well the difference in cultures. Often this plays out in how companies approach mobile device security. A company with a mature security approach may use a mobile device management system in order to enforce settings such as strong passwords, screen lockout, and storage encryption on smartphones that access, store or transmit company information. But at a start-up company, users may be accustomed to carrying their own smartphones and accessing company email and information freely, without any restrictions or policies brought to bear. These differences need to be documented early on in the acquisition process in order to develop strategy for introducing changes that will improve security at the acquired company.

Document, Track and Mitigate

If the acquisition moves forward and the target is purchased, then the findings from due diligence should be input into a risk register and tracked. At this point, a thorough risk assessment of the acquired company should be performed to identify the highest threats. Security experts can provide guidance on how to mitigate those threats.

- An example of an immediate threat would be a SQL injection attack on the acquired company's website, with exfiltration of customer data.
- Securing the perimeter and external-facing systems will be paramount.

It is only realistic to acknowledge that some form of connectivity between the acquired company and the parent company will be put in place, even if it is just minimal at first. The acquired company presents a side-door into the main corporate network.

Implement technology and network architecture to secure the network while allowing connectivity that is needed. Initial "Day One" connectivity may be limited to a secure portal or virtual desktops. However, when network connectivity is established for integration, carefully review firewall access control lists. Intrusion prevention controls and network monitoring should be enabled. Based on the risk assessment findings, apply technical solutions such as data loss prevention, user behavior analytics, and multi-factor authentication. Extend the organization's vulnerability management and incident response programs to include acquisition sites for coordinated detection and response.

Another facet of risk is how the acquired company may impact compliance. If the parent company is PCI compliant, then the initial due diligence and later risk assessments must look at how payment cards are handled at the acquired company. Finally, the target company itself may have valuable intellectual data and other assets that a hacker may seek to compromise. Identifying critical assets and securing them is a priority.

By addressing security governance at the beginning, at due diligence, and tracking risks throughout the integration process, companies can gain control over the information security and compliance risks in mergers and acquisitions.

Never underestimate the human factor. The security of data depends on employees who understand and carry out their role in protecting information.

- Security awareness and training should be extended to acquired companies as soon as possible, and in a manner that makes the training enjoyable and interesting.

One company set up tables in break rooms where users could stop by and participate in a demonstration of phishing or see examples of websites and fake antivirus programs that spread malware. For a more technical staff, running a packet analysis tool will show how easily unencrypted data (such as passwords in FTP or Telnet) can be captured and viewed.

Maturing the Process

To continue to improve security in Mergers & Acquisitions, organizations should document the information security activities from due diligence through network and system integration. Develop a playbook and maintain it as a living document, reviewed frequently. Further, establish clear ownership for information security at acquisition sites; clarify funding, lines of reporting, and shared responsibilities. Make M&A security a part of the organization's overarching information security risk management program.

In summary, mergers are a powerful driver of business growth, but bring a multitude of risks. Cybersecurity risk is part of that.

About NTT Security

NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies (Dimension Data, NTT Communications and NTT DATA) to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more about NTT Security or visit **www.ntt.co.jp/index_e.html** to learn more about NTT Group.

For more information please contact: US-info@nttsecurity.com or reach out to your NTT account representative.