GUIDEBOOK

Avoiding Cybersecurity Risk Through Enhanced Due Diligence

CrossCountry Consulting

TABLE OF CONTENTS

Avoiding Cybersecurity Risk Through Enhanced Due Diligence

Through mergers and acquisitions, companies can combine their strengths, gain access to new offerings and markets, and expand exponentially. Merging the assets of another company can also mean inheriting the systems, and thereby the strengths and weaknesses, of their IT infrastructure.

An acquisition of a new entity and its attendant technology and related security impacts represent a risk in terms of the additional threat vectors associated with the technology stack the new entity brings to the table. There are accumulated costs and effort necessary to resolve issues related to the acquired technology, which includes both the technology developed by and used by the target firm to enable business operations and/or as components of a solution being sold into the market.

Unfortunately, there have been too many instances of companies discovering IT security weaknesses the hard way: after an acquisition was completed. For example, Verizon's acquisition of Yahoo! and the disclosure of Yahoo's data breach misfortune carried a steep price: a $350 million discount off the original $4.8 billion agreed upon purchase price. Much like a strategic business plan, financial health, and legal liability, cybersecurity must be a priority during due diligence. Consider the following fictitious example of an acquisition gone wrong:

> *Ajax Software was a start-up rising star in the e-commerce world. They created a solution that took the internet payments world by storm. Recognizing their growth and the need to expand operations, the owners sought a strategic partner to help grow their business. Attracted by Ajax's existing market share and recognizing the synergy with their current web-based business, MegaWeb Corporation presented Ajax an acquisition offer. Owners of both companies agreed on the terms.*
>
> *Prior to the acquisition, the secret to Ajax Software's success was their proprietary, home-grown software platform and its simple integration with customer websites. With the acquisition complete, MegaWeb Corporation realized integrating Ajax's systems into theirs would be the most effective way to help both companies scale and beat competitors.*
>
> *Due to management, investor, and market pressures, MegaWeb Corporation conducted a shortened due diligence process to speed the acquisition. The next release of Ajax's platform would bring much-requested features and address a market on which they wanted to rapidly capitalize. The acquisition process was completed, and the "Mega-Ajax" platform was released to great fanfare and success.*
>
> *A year after the acquisition, a national news site published a story with headlines identifying Mega-Ajax as a victim of EvilX, an international crime syndicate that compromised Mega-Ajax's customer account database and corporate systems. In the days and weeks following the article, customers reported their identities and credit card information had been stolen. Worse still, as Mega-Ajax began to respond to these claims, their corporate systems were shut down by a devastating ransomware attack.*

Throughout this guidebook, we will explore MegaWeb's cybersecurity due diligence failings and offer suggestions for best practices in cybersecurity when exploring growth through a merger or acquisition.

CHAPTER 1

Assessing Cybersecurity During Due Diligence

What can your organization do to avoid a similar catastrophe and not end up like MegaWeb Corporation? Prior to entering into a business agreement with another entity, organizations need to identify incompatible business processes, potential integration problems, or unexpected liabilities through a due diligence process, such as those faced by MegaWeb and Ajax.

Traditionally, due diligence focused on business operations, legal concerns, and financial statements; as companies have become increasingly more reliant on data and technology, it is imperative to the security and reputation of an organization that cybersecurity posture, governance, and practices also be regarded. Consider the following when evaluating an acquisition or merger target. Depending on the nature of the business, some areas may pose a larger threat than others and require greater scrutiny. Throughout this guidebook, we will dive deeper into each of these areas.

Organization Cybersecurity Policies and Structure

Assessing alignment between the cybersecurity governance and structure of both organizations can smooth the process of integrating the security program of one company into another, highlight areas of weakness that need to be addressed in the formation of these programs, and prevent potential vulnerabilities or breaches down the line.

1. What policies are in place to govern the cybersecurity function?

What methodologies does the organization use to determine its cyber policies and governance structure? Does the organization benchmark its policies and capabilities against industry standard frameworks such as NIST Cybersecurity Framework, CIS Top 20, or the Cloud Security Alliance's Cloud Controls Matrix? Are there set policies and expectations for programs – such as patching, remediating vulnerabilities, identity management, and identifying risk – based on these frameworks?

2. Does the company, and the cybersecurity function, clearly understand the organization's critical assets and data systems?

How is this understanding incorporated into risk management decisions? Companies that have not identified critical assets and systems are less likely to make risk-informed decisions, which means their defense strategy, tool sets, and resource prioritization may not be focused in the right areas and will have less of an impact on the overall security of the organization.

3. How is the cybersecurity function structured and staffed?

Inadequate focus and leadership can impact the security posture of the company. For example, smaller startups may not have a Chief Information Security Officer (CISO), but it is important to, at a minimum, have a senior IT security leader who understands the architecture, engineering, data, and security pieces of their organization and products. This role may be outsourced to a third-party, provided the IT security leader has sufficient access and authority to be effective. Companies without a dedicated information security lead generally have a less organized, goals-driven cybersecurity program and therefore become more inviting targets for attack.

4. Is there an appropriate number of staff and delegation of duties?

Organizations that are understaffed or multi-tasking engineering and operations duties are more likely to miss or ignore issues and vulnerabilities.

5. How is leadership kept in the loop?

Good cybersecurity programs keep leadership informed on how it is monitored and managed. Does the cybersecurity leader have confidence that practices align with corporate policies? Is there a sense of complacency and resultant lack of oversight? How is leadership assessing themselves and setting future goals for security?

Organizational Approach to Cyber Threats and Vulnerabilities

Beyond ensuring cohesion with organizational strategy, structure, and governance, it is vital during the due diligence process to assess whether technical controls and prevention mechanisms are adequate.

1. What is their level of visibility into vulnerabilities?

Proactive identification and remediation of vulnerabilities is key to managing the attack surface of an organization.

- What is the method for identifying vulnerabilities within their IT environment?
- Are all endpoints running within their environment known?
- What are their metrics and Key Performance Indicators (KPIs) for tracking vulnerability management, and how quickly are they addressed?
- Do controls tie back to governance and corporate and regulatory policies?
- Are regular penetration tests performed on the environment to test controls?

2. Can they see attacks?

If a breach occurred, would they likely detect and respond rapidly and effectively before financial or reputational damage occurred?

- What tools, techniques and procedures are employed to monitor for attacks?
- Do these tools, techniques and procedures monitor endpoint security, email, web traffic, and DNS?
- Are insider threats monitored?
- Are the tools tuned appropriately to correctly identify malicious activity without generating excessive false positives?
- Are alerts aggregated and monitored?
- Is there adequate monitoring coverage of the environment during off-business hours and holidays?
- Do they perform “Red Team” or “Adversary Emulation” assessments? These types of exercises mimic the stealthy attack of a real adversary and are important for evaluating their IT security program’s ability to detect and respond to attacks.

3. How do they respond to attacks?

According to an IBM Security report[1], mature incident response plans, testing, and teams can reduce the cost of a breach or attack by an average of $2 million.

- Do they have an incident response plan?
- Do they have a Security Operations Center or managed service provider that will act immediately to a potential attack or threat?

4. How are threats modeled? Do they perform any other proactive measures to anticipate potential attacks?

Identifying likely threats and modeling attacks allows an organization to understand their attack surface, how adversaries see them, and attempt to exploit them. Are countermeasures in place, and have they mitigated the level of residual risk?

- Do they conduct threat modeling exercises periodically?
  - Threat modeling is typically a tabletop exercise.
  - Adversary Emulation, a hands-on assessment, need to be performed to mimic the behavior of a real adversary. This Adversary Emulation team enacts the modeled threat and measures the organization’s response.

[1] https://www.ibm.com/downloads/cas/QMXVZX6R?lnk=STW_IN_CLP_L1_TL&psrc=OPT&pexp=mob&lnk2=ar_DataBreach

5. How do they monitor geopolitical threats that can cause a spike in cyber-related activity?

Maintaining a clear understanding of threat intelligence and changing international events will impact threat landscapes and allows organizations to proactively update their cybersecurity strategy.

- Is the organization aware of their threat landscape, particularly from a geo-political perspective?
- Does the company stay up to date on world news and events, and understand how they impact their cyber and organizational risks? For example, sanctions on Iranian banks often correlate to increased cyber attacks on financial services infrastructure.
- Do they have a threat intelligence program? If so, does it provide relevant, timely, and actionable information on the threats specific to their organization? Programs that provide too much data without relevance are generally ignored.

Addressing Privacy and Regulatory Issues

During the due diligence process before a merger or acquisition, organizations should understand the types of data that they will inherit, respective sensitivity levels, and the applicable regulations with which they will need to comply.

1. How do they stay on top of the changing regulatory landscape for both privacy and cybersecurity?

Understanding requirements set forth by the constantly evolving U.S., state, and international privacy laws is critical for organizations to maintain compliance.

- How are regulatory requirements, such as those from federal, state, and international privacy laws, tracked and inventoried?
- How do they measure and monitor compliance against the regulatory requirements?
- Have they had any previous information requests from regulators wanting to examine their operations?
- Have they entered into any legal agreements with regulators required to correct their handling of data or other operations?

2. Are they aware of the sensitive regulated data within their environment and the repercussions of a breach?

Privacy regulators are honing in on companies that fail to protect data and levying fines worldwide. Organizations need a strong understanding of the data they collect.

- What categories of data are collected?
- Do they understand their data lifecycle? How is data collected, used, shared, retained, and destroyed?
- Have they implemented a data mapping strategy to identify where data is stored, internal data owners, and access controls to prevent unauthorized access or disclosure?
- Do contracts with vendors who process their data include strict requirements setting forth the instructions, duration, and types of data subject to processing, and the requirement to inform the company of any breaches without delay?
- Have they had any previous data breaches that met the legal threshold to notify regulators or customers?

3. Is there an audit function providing an independent evaluation of the control environment and adherence to regulations/ law?

If so, is that function internal or outsourced? What standards and frameworks, in addition to regulations, are used for this evaluation? How is the organization managing timely remediation of issues identified?

Supply Chain Risks

An organization's cybersecurity is only as strong as its weakest link. During a merger or acquisition, an organization linked to third parties with known vulnerabilities or security issues is likely to pass on potential attack paths. Ultimately, performing your due diligence to ensure an effective approach to supply chain security is vital.

1. Is there a third-party or supply chain risk function that addresses the risk that third parties pose to the reputation and security of the company?

- Does the organization have a good grasp of all the third parties that provide products or services, or partner with them?
- How do they perform due diligence prior to onboarding new third parties or renewing contracts? Do they assess and rank third parties by risk?
- How do they perform ongoing monitoring of third-party risks and compliance with established cybersecurity requirements?

2. How is leadership informed and kept aware of the various risks posed from suppliers, both new and existing?

- How are risks managed, monitored, and reported to leadership?
- Do they include risk factors like those in their third-party scorecards and procurement processes?

Failing to assess the cybersecurity program of a mergers and acquisitions target exposed MegaWeb Corporation to tremendous financial, data, and reputational damage. By asking these questions, organizations will better understand the threats and vulnerabilities of the acquisition or merger candidate.

CHAPTER 2

Determining Organizational Maturity through Cybersecurity Policies and Structure

During the mergers and acquisitions process, thorough cybersecurity due diligence is vital. Ideally, the structure and governance of both companies should be as similar as possible to allow a more seamless integration of the security program of one company into another. This will also help to avoid a potential disaster – such as a breach or unknown data protection weakness – down the road that may destroy the financial security and reputational image of the company. Finding such structural and governance alignment upfront is alarmingly rare.

The first key areas that our fictional company MegaWeb Corporation should have evaluated before finalizing the acquisition of Ajax Software are their cybersecurity structure and policies. Mature and effective security programs are governed by strong, well-informed leadership and concise, well-understood policies. These types of programs are enabled by full-time security professionals focused solely on the security of customer data and company systems vital for conducting business.

1. How did the Ajax Software leadership view cybersecurity?

Before any merger or acquisition, it is important to ensure that the cybersecurity functions of both organizations are given appropriate levels of attention and funding. This begins with leadership. Companies that support security objectives from the board and C-suite create a better security culture than those whose leadership view security as simply a check box and expense.

Had MegaWeb validated the level of attention and funding that the cybersecurity function at Ajax received from leadership, they would have seen that security was considered irrelevant and red flags would have gone up.

2. Did Ajax have a Chief Information Security Officer (CISO) or designated security authority?

Most companies in today's world have some form of a cybersecurity program. But who prioritizes needs, decides to whom to delegate tasks, sets future goals, or champions security culture? In well-established cybersecurity programs, this person is the CISO or an equivalent role, while smaller firms may utilize a versatile, multi-hat individual such as a senior IT/security leader. During the merger and acquisition process,

Companies that do not have a security leader who is tasked with prioritizing cybersecurity generally do not have well-defined security goals and standards.

MegaWeb Corporation should have verified that Ajax had appropriate security leadership, or at least a designated and sufficiently trained cybersecurity authority.

Companies that do not have a security leader who is tasked with prioritizing cybersecurity generally do not have well-defined security goals and standards. This can lead to unseen and unanticipated security gaps.

3. Did Ajax have proper cybersecurity staffing for the size of the company?

All departments within an organization compete for budget and resources; it is the nature of the corporate world. However, does a firm want to gamble with such a risk, knowing the potential consequences associated with a breach?

With Ajax, they risked losing customer payment data in this event. Therefore, it should have been essential for MegaWeb Corporation to examine the number of cybersecurity staff that Ajax employed. Mature, well-functioning cybersecurity programs have a healthy number of staff, solely dedicated to the mission of protecting customer and employee data and company IT infrastructure. Requiring them to split time between security and other tasks (such as development) is common within start-up culture. This practice becomes riskier as a company matures and sales and market presence increase.

What exactly is considered a healthy number? Security teams should be staffed to ensure that organization objectives can be met without a large amount of backlog, and emergency and high-priority turnaround items are quickly addressed. Organizations unable to find the appropriate talent or expertise may consider the option of hiring contractors or a managed service provider to assist.

4. What cybersecurity policies were in place?

Policies are a vital part of a cybersecurity program and should set security criteria that is well-communicated and enforceable. These policies can stem from a broad, company-wide acceptable use policy for company workstations and devices, to a more granular exposure management policy for server administrators to ensure identified vulnerabilities are remediated in a timely fashion. Depending on the industry and the organization's requirements, industry-leading standards and frameworks – such as NIST Cybersecurity Framework, CIS Top 20 Security Controls, ISO 27001 and 27002, or COBIT – should be applied.

STANDARD/FRAMEWORK	DESCRIPTION
NIST Cybersecurity Framework	Standards, guidelines, and best practices to manage organizational cybersecurity risk
CIS Top 20 Security Controls	A list of highly prioritized best practice guidelines for effective cybersecurity controls organizations should put in place to block or mitigate common attacks
ISO 27001/2	Best practice recommendations for cybersecurity management
COSO	Establishes a common language and foundation for organizations to assess and oversee risks from a holistic perspective
PCI Data Security Standard	A cybersecurity standard detailing security control requirement to protect cardholder data and decrease credit card fraud

MegaWeb Corporation should have examined Ajax's current cybersecurity policies and conducted an audit or risk assessment to ensure that they matched operations in practice. Had MegaWeb Corporation not been satisfied, they could have ensured that Ajax addressed gaps or shortcomings before the acquisition or addressed their concerns as part of the integration plan. Ajax staff smoothly transitioning into what was expected as part of a mature security program would have brought peace of mind to MegaWeb.

5. What are the company's critical assets?

Does the company and the cybersecurity function clearly understand the organization's critical assets and data systems? How is this understanding incorporated into risk management decisions?

Depending on maturity level, most organizations should have conducted a risk or "crown jewel" assessment to identify their critical assets, data, and systems. Understanding these assets allows cybersecurity leaders to focus resources and priorities on the defense of what matters most, and building a cybersecurity program focused on strategies with the biggest impact and return on investment for organizational security. A clear understanding helps ensure business continuity and cyber risk management decisions are made with threat-informed intelligence and risk prioritization in mind. Companies that have not identified critical assets and systems are likely to be making poor risk-informed decisions; their defense strategy, tool sets, and resource prioritization are unfocused and have less impact on overall organizational security.

MegaWeb Corporation should have required Ajax to conduct a crown jewels assessment, list their critical assets, and outlined how their security programs were structured to protect them. If Ajax could not identify these assets, it would have indicated to MegaWeb that a deeper evaluation of security policies and procedures was needed prior to the companies' systems integration. The vulnerabilities that later led to the breach would have been identified and patched before damage was done.

Companies who have not identified their critical assets and systems are less likely to be making risk-informed decisions.

6. How was leadership kept "in the loop?"

It is important for leadership to drive cybersecurity within their organization. This begs the question: How do they evaluate the effectiveness of their efforts? What should MegaWeb Corporation have done within the cybersecurity program at Ajax before acquiring the company?

Within any mature cybersecurity program, leadership should require the CISO or equivalent role and the leaders within their organization to develop Key Performance Indicators (KPIs) that provide a holistic picture of the state of the program, as well as progress against future short- and long-term goals.

If Ajax had developed a security program, perhaps MegaWeb would have seen that Ajax was not remediating vulnerabilities in a timely fashion, or that their staff was susceptible to phishing. Perhaps Ajax was missing deadlines on implementing their new Security Event and Information Management (SEIM) tool to monitor their infrastructure? Objectives and timelines help leadership drive accountability and set goals, a requirement in the M&A process.

Conclusion

Much can be determined about an organization's security posture and maturity by viewing their policies and structure. Had MegaWeb Corporation included cybersecurity in the due diligence process, they may have discovered that it was not an Ajax leadership priority and would have found that Ajax did not have a CISO or equivalent role driving security efforts forward. MegaWeb would have seen the poor security program that Ajax reported on vulnerability management and phishing susceptibility, and that developers were multi-tasking security efforts. While there is never a 100 percent guarantee within the cybersecurity world, MegaWeb would have been better off ensuring that Ajax had a strong cybersecurity structure, effective policies, and dedicated management.

CHAPTER 3

Technical Solutions for Organizational Resiliency to Cyber Threats and Vulnerabilities

While strong policy and governance are vital to an enterprise's security posture, adequate technical solutions that address security risks should be implemented. This is particularly important when sensitive or regulated data needs to be protected from a breach, or key products and services must be available to customers. To address the attack surface malicious actors will exploit, technical security solutions should be implemented throughout the entire IT stack, with additional specialized solutions in place to limit the scope of the breach.

Our fictional company MegaWeb Corporation needed to spend time taking an in-depth look into the security configurations and solutions of the payment processing system, as well as the supporting infrastructure that Ajax had developed. As soon as MegaWeb completed the acquisition, the vulnerabilities that once belonged to Ajax now belonged to MegaWeb.

While limiting financial and other types of operational risk that often garner more attention from leadership, it is equally important to curb the potential security vulnerabilities to your organization. What could Mega Web have analyzed to ensure their risk acceptance was as low as possible?

1. Did Ajax require multi-factor authentication to be deployed everywhere possible?

One of the easiest ways to prevent unauthorized access to customer applications and platforms, and supporting infrastructure on the backend, is to enforce multi-factor authentication (MFA). MFA requires a user to provide both something they know (e.g., a password or pin) with something they have (e.g., a smart card, SMS or email code, or biometric marker such as a fingerprint, retina scan, or voice analyzation).

Alexander Weinert, Director of Identity Security at Microsoft Corporation, revealed at the 2020 RSA conference[2] that 99.7 percent of compromised Azure (their cloud computing service created for building, testing, deploying, and managing applications and services through their data centers) accounts did not employ MFA, relying simply on password authentication.

One of the easiest ways to prevent unauthorized access to customer applications and platforms is to require the use of multi-factor authentication.

[2]https://www.youtube.com/watch?v=B_mhJO2qHIQ 2/28/2020 Speech by Alexander Weinert, Director of Identity Security, Microsoft Corporation

Had Ajax employed MFA on its customer portal as well as the backend infrastructure and applications, the attackers likely would have been thwarted before the attack even began.

2. What if Mega Web had ensured Ajax employed encrypted data at rest and in transit?

Another key method to prevent unauthorized access to customer and organizational data is to ensure strong forms of encryption are used from the time it is generated to the time it reaches its storage location. When a customer supplies data to an application, it needs to be encrypted in transit, which prevents an attacker from capturing it en route, preventing man-in-the-middle attacks to your organization's infrastructure.

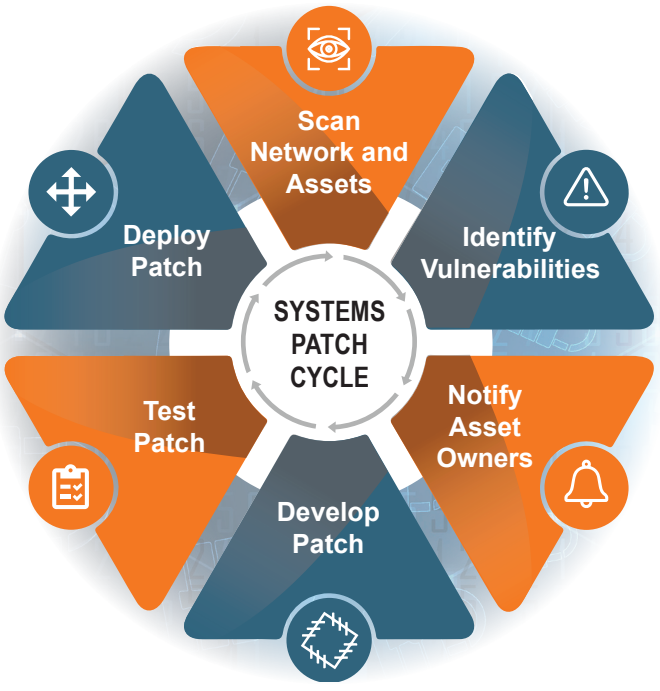
Transport Layer Security (TLS) version 1.3 is the strongest form of transit encryption available (although most web applications currently use version 1.2, which is still considered secure). Websites that require users to enter credentials should use HTTPS (the secure version of HTTP), which ensures that credentials are encrypted prior to passage through the internet for user authentication; without it, an attacker can see your passwords in clear text.

Once data reaches its destination, it will be stored within a database. In the event an attacker can access the contents of a database server, it is vital they use AES-256 bit encryption, currently the strongest commercially available, to prevent them from viewing sensitive customer data. Because weaker encryption protocols such as RC4 and 3DES can be cracked, it is insufficient.

Had MegaWeb ensured Ajax employed encryption in transit and at rest, the attackers would have been prevented from obtaining the credentials that compromised the customer databases and corporate systems.

3. Did Ajax scan systems for vulnerabilities and patch them regularly?

Attackers are constantly searching for exploits to use on systems, as well as the software and services that run as part of those systems. Often, they are successful at their attempts once an exploit is discovered, which is why it is essential that organizations properly manage vulnerabilities and patch software and hardware. As a best practice, organizations should scan their internet-facing infrastructure on a weekly basis,



and internal systems bi-weekly. Popular scanning tool brands such as Nexpose, Qualys, and Tenable will rate the urgency of the vulnerability and often provide a method for its remediation.

Critical vulnerabilities should be patched immediately, and high vulnerabilities within a week to limit the window an attacker will exploit it. Infrastructure should also undergo regular, third party-driven patching of firmware and software to ensure that systems are consistently running up-to-date versions that often remediate exploits or vulnerabilities. Microsoft's "Patch Tuesday" is a good example of third party-driven patching.

Had MegaWeb validated the vulnerability management posture of Ajax prior to integrating Ajax's systems into their infrastructure, the exploit likely would have been remediated before the attackers could take advantage.

4. Did they ensure that their logs were configured and analyzed for threats?

To properly respond to a potential attack, organizations must ensure they have information about what is occurring and acknowledge anomalies that appear in their normal activity. To do this, businesses should install Security Information and Event Management (SIEM) software (such as LogRhythm, Splunk, ArcSight, and QRadar) that has the capability to ingest and analyze the logs from the system stack, as well as monitor the infrastructure for indications of or attempts at compromise. To ensure a quick response and to contain any potential threats, your organization should have on-call staff, ideally 24/7, that monitors and analyzes alerts generated by the SIEM tool.

Had MegaWeb ensured that Ajax configured their infrastructure for monitoring via SIEM, the attack would have likely been detected and contained more quickly, minimizing the impact.

5. Did they attempt to penetrate their infrastructure and applications through tests?

It is critically important to gauge the effectiveness of your security controls and application development security practices. This can be accomplished through penetration testing, when a skilled tester is tasked with finding and validating vulnerabilities that would allow an attacker access to the application or associated infrastructure and the sensitive data contained within. Vulnerability scanning alone often results in false positives; penetration testing can validate which ones are exploitable and help prioritize the vulnerabilities for remediation.

As a best practice, organizations should employ an annual penetration test on all critical customer applications/ platforms, including the network. This will help organizations identify weaknesses in code, infrastructure misconfigurations, or security gaps that need addressing. These are better found by a skilled "good guy" versus a skilled attacker. Once discovered, the tester can work with your organization to remediate the findings.

MegaWeb should have ensured that the Ajax platform and network had received annual penetration tests before integrating it into their own infrastructure, enabling the “good guy” to find the exploit before the attackers could.

Conclusion

Some organizations see investments in security technology as an impediment and a delay in go-to-market for new products and features. This could not be further from the truth. Investing in security protects customers from the headaches associated with a breach and organizations from the negative financial and reputational impacts that cost more than the original investment. Leadership must stay on top of the latest threats within the cyber world and invest in technology to prevent those threats from occurring.

We see what happened when MegaWeb did not perform the proper due diligence on Ajax’s investments in security technology. It cost them more than if they had taken the time to properly evaluate and remediate any gaps. Slow down and make sure the proper security technology is implemented. Your customers and organization will thank you for it, and your merger or acquisition will be better positioned for success.

CHAPTER 4

Addressing Privacy and Regulatory Issues Before Integrating Company Systems

In recent years, the adoption of the General Data Protection Regulation (GDPR) in the European Union (EU), the passing of the California Consumer Privacy Act (CCPA), and several other state-level regulations in the legislatures across the United States have brought privacy regulation into the spotlight. These regulations have come with additional reputational and regulatory risk (e.g., fines), increased consumer rights, and an enhanced focus on how companies use data as a commodity.

Due in large part to public and damaging privacy scandals such as Cambridge-Analytica's misuse of social networking site Facebook's profile data or the breach of credit reporting agency Equifax consumer information, the public is asking more than ever where and how their personal information is being used.

When evaluating potential acquisition or merger of target organizations, it is important to scrutinize the risks and benefits of large data sets that contain personal or sensitive information.

While privacy policies will not stop a breach from happening, looking at applicable controls an organization has in place during the due diligence process will serve to make the integration of systems more efficient, highlight any trouble spots where response to regulatory frameworks and requirements do not align, and identify missing controls before integrating disparate systems.

1. What is the geographic scope of the target organization? How does this change the regulatory landscape?

Based on the physical location of the organization and types of data they collect, process, transmit, and store, an acquisition target may be simultaneously subjected to multiple state, federal, international, and industry-specific privacy and compliance standards and laws. As more states and countries consider passing legislation, the complexity of the privacy regulatory landscape continues to shift. If there is a privacy program, this requires organizations to swiftly react and comply to newly scoped legislation with varying degrees of change and impact.

When assessing a target organization, it is paramount to confirm that the cybersecurity program and controls consider the full geographic scope.

Likewise, review your own compliance function to ensure that your organization is ready to handle the added complexity that the acquired company will bring.

Had MegaWeb assessed the related privacy and regulatory requirements of Ajax, they could have identified discrepancies with their own regulations and would have been able to ensure their policies aligned prior to sharing data and systems.

2. What did the target organization's privacy policy state during the collection of personal data?

The U.S. Federal Trade Commission (FTC) has published clear guidance communicating that regardless of a merger or acquisition, organizations must continue to honor the promises made to consumers in privacy policies. The FTC considers failure to comply with published privacy policies a violation of Section 5 of the FTC Act, which bars unfair or deceptive acts in commerce.

When assessing a target organization, it is essential to confirm any disclosure or new uses of personal data will follow promises made about the treatment of personal data in the target company's privacy policy. Any new uses of acquired data must be consistent with the purposes of processing described to consumers when personal data was initially collected, and until it can verify uses are consistent (such as providing a similar product or service), isolate the data you know you have been collecting legitimately from the newly acquired data.

Before the integration of data and systems, determine what consumer-facing actions, if any, must be taken to ensure the data can be shared and used. Actions may include providing notification to consumers of their right to opt-out of having their personal data shared, obtaining opt-in consent from consumers to share their personal data, or any other actions that allow you to demonstrate to regulators the privacy policy provided at the time of collection was sufficient notice for the future sharing of personal data, and your uses are consistent with the purposes of processing described at the time of collection.

Had MegaWeb thoroughly evaluated the Ajax privacy policy to ensure their proposed uses of Ajax customer data were consistent with promises made to Ajax customers, they would have avoided legal and regulatory risk by ensuring policies were aligned prior to integrating data and systems.

3. Does the organization share personal data or other protected information with third parties? Do they have an adequate process to implement security and privacy safeguards over that data transfer?

As with related IT and cybersecurity risks, the greater number of third parties involved in the use of personal or other sensitive data, the more complex compliance with privacy regulations becomes. Some legislative bodies, such as the European Commission and state of California, have provided specific instructions and definitions around who qualifies as a third party and what requirements need to be in place to meet the letter of the law. Protecting in-scope data necessitates a comprehensive and mature process, inclusive of legal, compliance, IT/cybersecurity, and privacy teams. During due diligence, ensure that the data protection policies and procedures in place are adequate. Otherwise, you may find your organization inheriting

significant risk. Moreover, if the acquisition target does not have a robust data protection program in place, ensure that the integration plan includes strengthening this function.

If MegaWeb had evaluated the data protection policies and technologies at Ajax, they could have identified security or privacy gaps in data handling processes that needed to be addressed before integrating their systems and exposing customer data to vulnerabilities.

Organizations should maintain robust data governance plans, data architectures, and detailed data flows and maps.

4. Does the target organization have a process for identifying, classifying, and protecting data based on sensitivity or regulatory requirements?

Many organizations struggle after a breach because they do not have existing analysis and robust data mapping capabilities in place to proactively identify data in use or storage. Additionally, data is collected at such a rapid pace and volume that keeping track of what the organization currently possesses is an ongoing challenge. With potentially dozens of "data owners" and disconnected systems, it is difficult to identify what has been collected, where it is stored, how it is being used or processed, and if proper notice has been provided to customers.

During due diligence, review the data classification process and confirm that the organization has a good understanding of what it uses and stores on behalf of customers. Organizations should maintain robust data governance plans, data architectures, and detailed data flows and maps that can demonstrate where sensitive elements exist in the environment, and who is responsible for its maintenance.

If Ajax had strong data governance policies in place, it could have driven increased protection and monitoring strategies around customer and other sensitive information that would have protected it against attack or rendered it unreadable even if it were improperly accessed.

Conclusion

As unique data protection regulations become more common and increase the number of requirements to protect sensitive elements, organizations must consider the amount they store and what is shared with third parties, which is critically important during any merger or acquisition. Privacy and data governance capabilities should be an area of focused attention when conducting due diligence on a potential target organization and throughout the integration process.

CHAPTER 5

Addressing Supply Chain Risks During the M&A Due Diligence Process

An equally important area for companies to examine as part of their M&A process is supply chain risk, what it is, and how it pertains to cybersecurity. Most importantly, why does it matter to the mergers and acquisitions process?

Within the context of cybersecurity, supply chain risks are those posed to your organization that derive from third-party suppliers (e.g., the typical “raw material” providers many manufacturers depend on, or a piece of third-party software on your systems or hosted by a third party in their cloud that you may rely on for key aspects of your business). Whoever they are, third parties provide products or services your business depends on to operate.

Third parties introduce a wide variety of risks to an organization which need to be planned for. These risks are generally unique to individual third parties, but one factor is universal: They can have devastating consequences to your organization’s reputation and bottom line.

Suppliers provide several avenues for attackers to access your network and data or disrupt your organization. There are two main scenarios: first, loss of service for critical applications and services; and second, loss of proprietary data, whether from customers, employees, or other third parties. Both pose serious consequences to an organization.

Faced with market and investor pressure, MegaWeb neither assessed the suppliers employed by Ajax, nor determined how closely Ajax themselves evaluated their security. By cutting these corners, MegaWeb exposed itself to both catastrophic scenarios.

So, what needs to be addressed within the M&A due diligence process to ensure neither happens to your organization?

1. Did Ajax have a third-party inventory?

When reviewing Ajax’s cybersecurity supply chain risk management processes, Mega Web needed to first understand what third parties they relied upon. What third parties had access or transmitted data to Ajax systems, data, and facilities? What Ajax data resided in third-party systems? Which third parties provided critical or strategic services to Ajax or interacted directly with customers?

To answer these questions with a high degree of certainty, Ajax would have needed a repository listing all third parties and their detailed interactions by the company. There would need to be

documentation of the operational and reputational effects of a third-party breach, and the consequences a loss of service would have on the organization.

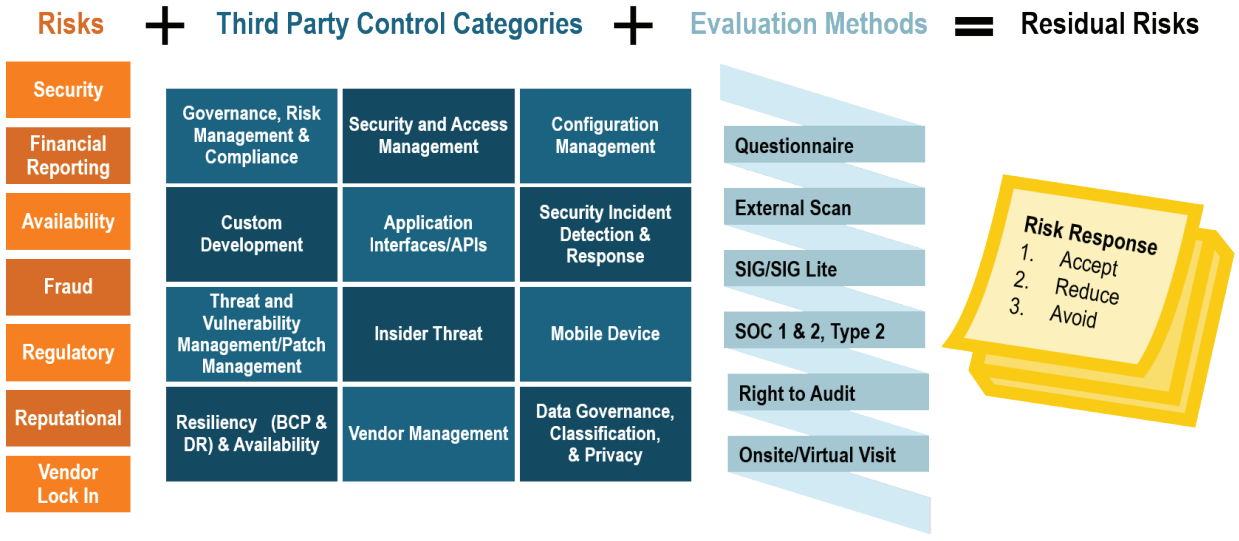
Had this been available, MegaWeb Corporation would have understood factions they would be inheriting as third parties; the risks each supplier presents; the risk mitigation, liability, and indemnification built into third-party contracts; and if they would want to keep those relationships, renegotiate, or terminate contracts.

2. Did Ajax understand who their critical suppliers were?

Beyond a vendor repository, MegaWeb should have ascertained Ajax knew who their critical and strategic third parties were. Understanding which ones provide business critical and strategic services, which connect to sensitive data and systems, and which have access to internal networks is integral to an effective cyber risk management strategy. Once identified, those third parties with higher levels of access, or who provide business critical services, can be prioritized based on urgency and security requirements for contracts and agreements. Had MegaWeb determined whether Ajax performed these leading practices around their critical suppliers, they would have been better able to assess the level of risk posed by Ajax's third-party suppliers prior to connecting their systems.

3. Did Ajax conduct due diligence on its suppliers?

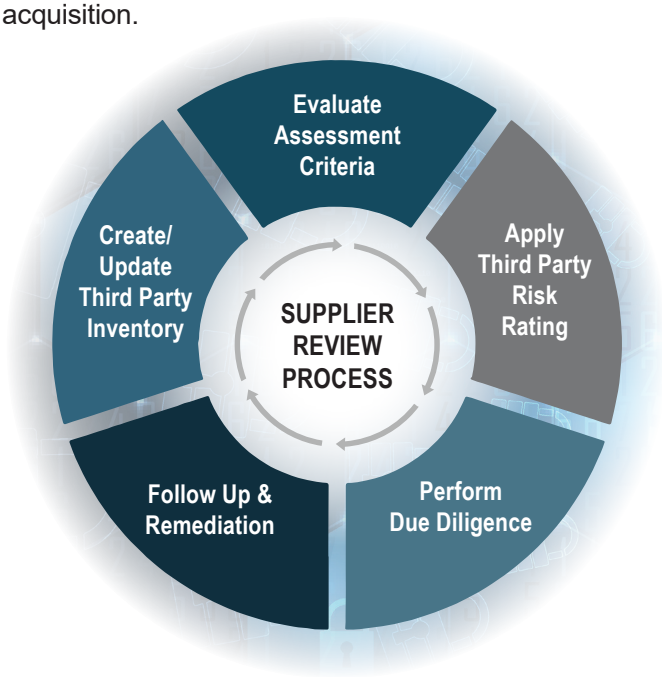
Mega Web Corporation should have determined whether Ajax examined their suppliers' security postures, and if they met a high level of expectation. A key aspect of cybersecurity supply management is conducting periodic due diligence and monitoring reviews to assess the controls that are in place over inherent risks to determine what residual risks impact the organization. If MegaWeb had been able to determine what third parties Ajax considered risky through these types of reviews, whether the risks were potentially impactful, and what risk mitigation strategies were in place during the acquisition integration, it would have helped them to make key business decisions during the acquisition process.



4. Did Ajax require third parties to remediate findings and inadequacies?

Third-party reviews serve a critical purpose: drive down risks posed by the third parties and their services and products. During these reviews, uncover risk items the organization is not willing to accept and will need to be addressed prior to the acquisition.

Best practice organizations not only conduct these reviews, but also have established processes to monitor and manage identified findings, in accordance with language included in contracts with each third party.



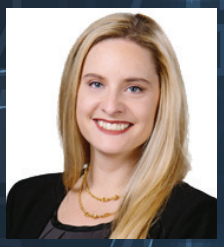
Had MegaWeb Corporation validated that Ajax was tracking remediation requirements for third parties, established remediation timelines with third parties, and ensured that they were following up on the open items until resolved, these deficiencies would have been corrected. They would have been comforted to know that Ajax demonstrated a requirement for their suppliers to meet an equally high standard of security.

5. How was Ajax leadership informed of and kept aware of third-party risk?

Lastly, MegaWeb should have looked at how leadership was kept informed of third-party risks, and the associated consequences of a breach or loss of service. Developing Key Performance Indicators (KPIs) and dashboards on third-party risk levels would have helped to ensure that Ajax leadership had a clear picture of the third-party risk landscape, such as having quarterly executive board reporting (i.e., report out the number of transfer pricings [TPs]: new, terms, those in due diligence, key risks if any), monthly risk committee meetings, an escalation process defined to obtain appropriate approvals when risks are not adequately remediated, and review of contract terms to determine if the third-party risk was adequate (i.e., a formal risk acceptance process). Had this been the case, MegaWeb Corporation would have gained assurance of the overall effectiveness of the third-party risk management program.

Conclusion

Organizations can address possible internal controls, but if they are not approaching third-party risk with the same level of urgency, they are missing one of the main attack vectors we see in cybersecurity today. If MegaWeb Corporation ensured that Ajax had an effective third-party risk management program, they could have identified risky third parties that led to their compromise, made sure deficiencies were addressed, and severed ties with the third party before suffering downtime, loss revenue, and reputational damage.



Cameron Over

Cyber & Privacy Practice Lead

cover@crosscountry-consulting.com

703.899.6486

Sean Sinclair

Director, Business Transformation

ssinclair@crosscountry-consulting.com

207.831.5855

CrossCountry Consulting is the trusted partner and expert advisor to leading organizations. We help our clients transform their finance, accounting, human capital management, risk, operations and technology in order to effectively prepare them for complex change, optimized performance and accelerated business growth.

CrossCountry Consulting