The Importance of Cybersecurity Due Diligence for an M&A Deal

By Roland L. Trope

This chapter will discuss the importance of cybersecurity to an M&A deal and provide counsel with background that may help facilitate discussions with the client before undertaking a cybersecurity due diligence of a target.

1. Cybersecurity Challenges

Cybersecurity is about protecting a company’s digital assets and its brand. Yet implementing cybersecurity often presents unusual challenges, regardless of the size of the company and the scale of its dependence on digital information and processes. Uncertainties pervade the landscape.

Digital information, systems, and communications are critical to all businesses. Virtually all of a company’s daily transactions and key records are created, used, communicated, and stored in electronic form using
networked computer technology. Likewise, virtually all information on which a company relies to conduct its business, manage its finances, run its production machinery, and control its operational systems is created and stored in digital form.

Corporate dependence on electronic records and a networked computer infrastructure introduces vulnerabilities that can lead to significant harm to the business and its stakeholders. Creating, processing, communicating, and storing corporate information in electronic form greatly increases the potential for its unauthorized access, copying, use, disclosure, and alteration. It is no longer prudent in today’s environment to assume that an enterprise’s networks and digital assets can be completely secure against cyber intrusions, whether from disloyal insiders or outside adversaries.

Increasing an enterprise’s defensive measures may reduce the ease with which intruders gain unauthorized access, but to date no defensive measures provide completely reliable safeguards. The more iconic the enterprise or valuable its digital assets, the greater the probability it will draw the attention of intruders. And increasingly, the intruders have the skill, computing resources, malware tools, and stealth needed to gain access undetected and to operate maliciously within the enterprise for an extended period. No enterprise is immune from cyber breaches.

Moreover, modern enterprises are continuously under siege—from both the outside and from within. Remarkably few enterprises have a reliable grasp of how often their digital assets have been accessed or of potential intruders’ objectives. An increasing number of reported incidents reveal an intrusion that proceeded undetected for weeks, months, and sometimes years. Whatever harmful intent the intruders have, the stealth of their operations makes cyber defenses appear effective only at requiring the would-be intruders to use their best methods, such as advanced persistent threat (APT) attacks, against which few, if any, enterprises have any reliable defense. At the same time, new sophisticated forms of APT are emerging such that almost all attacks are “surprise attacks”—they begin and end before the target knows it has been hit, causing new and unfamiliar damage such as information leakage or data modification, the damaging consequences of which may be misunderstood for months before the target can trace the operational effects to the cyber cause.

Defenders of enterprise security thus operate at immense disadvantages. An attacker need only find one unguarded gap, vulnerability, or exposed endpoint in an enterprise’s defenses. The defender, however, must secure
every vulnerability, new ones as soon as they are discovered, and all the vulnerabilities that newly adopted technologies add as well.

Furthermore, the primary cyber threats faced by enterprises have rapidly evolved. The primary threats are no longer “viruses created by hackers . . . mostly interested in mischief or vandalism” (as in the 1980s and early 1990s), nor “botnets, spam, and dark markets for stolen credit card numbers” (as in the late 1990s and early 2000s), which used the same form of attack simultaneously against multiple targets. Some form of defense against those types of threats eventually became effective. Security software became available to “track the patterns of attack and stop bad code from getting inside a network. Despite the occasional breach, it did a reasonably good job.”

Now, however, governments and other well-resourced organizations have made significant improvements in the destructive power and stealth of cyber attacks. Such organizations have recently sponsored sophisticated, customized attacks on specific targets—Sony Pictures, the Democratic National Committee, the US Office of Personnel Management. Because bad code is [often] custom-written for each assault, the hackers don’t leave patterns of attack, which means the core design principles of prior-era security software no longer apply. This has shifted the balance of power to the attackers.

As a result, the means for conducting a successful intrusion—and the means for remotely compromising digital assets (by misappropriation, modification, degradation, disruption, or destruction)—have become more powerful and widespread. Hence, improvements in cyberadversaries’ tools continue to outpace improvements in cyber defenses.

Understanding what attacks can do to data is crucial to understanding why companies so often find themselves unaware that they have been successfully attacked or, after discovering what has happened, may be ill-informed as to the significance and consequences of the intrusion.

2. Id.
For M&A cybersecurity due diligence teams, it is important to assess whether a target company has the means to know five fundamental facts about the target’s experience with any cyber incidents.

First, what data might the attackers have gained (or still be gaining) access to? The basic tool that a target company needs in order to ascertain that is an intrusion detection system or IDS. An IDS alerts the target that unauthorized entry has been made into its networks, or that an unauthorized person has accessed its files. But IDS does not identify what the intruders did. Did they read files? Did they change permissions so that they could log in and appear authorized? Did they make copies of customer lists? Or worst of all, did they modify data? IDS does not answer those questions. Instead, by alerting the target to an unauthorized entry or intrusion, the IDS puts the target on notice that each of those actions might have, or might soon be, carried out.

Second, what data might the attackers have viewed and exfiltrated copies of? It’s possible the attackers saw something they wanted, such as the company’s password file. If that was available to any intruder without having to overcome any other defense, the target would need to have its personnel immediately change their passwords. But knowing whether the attackers may have removed copies of data requires the use of a data protection program. Such program helps to determine whether data left the target’s computer networks without permission. It should also assist in determining whether the data was encrypted and where it was removed from, which may be quite significant if say, the data came from the CEO’s or CISO’s files.

Third, what data might the attackers have changed? This is often the real bugbear. Did the attackers modify data contained in certain files and if so, what changes did they make? This is far more difficult to determine than whether the attackers accessed or removed a copy of a file’s data. For example, in the case of a defense contractor, the attackers might not only have removed a copy of the manufacturing design for a stealth fighter’s aileron, but also modified the target’s copy so that further use of that design data will embed defects or flaws that were not in the original design. No one at the target will know that has happened unless they are extraordinarily familiar with the data, and happen to make a close comparison of the currently active file with a back-up that is reasonably good, i.e., that the attackers did not alter. But given that sophisticated, stealthy attacks may continue undetected for months or years, how far back
does a target’s personnel have to go to obtain a reasonably good and reliable back-up in order to ensure the copy is of the original design and not of the design as modified by the attackers? Even small, seemingly insignificant changes to critical data can have catastrophic impact on products and on users. A health care example illustrates how small changes in data can cause large, widespread effects:

- If attackers access blood type data for company, diplomatic, or military personnel, they may make an inobvious change such as modifying each patient’s blood type letter (e.g., Type A to B, Type B to AB, Type AB to O, Type A to O).
- The blood type data may look fine (e.g., it still expressed as one of the four alphabetical blood types), but everyone of those persons who may thereafter need blood in an emergency and whose blood type is provided by the file that the attackers modified may get a harmful transfusion of the wrong blood.
- Result: an ABO incompatibility reaction, causing the patient’s immune system to produce antibodies against any blood antigens the patient does not have in his or her own blood; treatment will try to prevent, but may not avert, kidney failure, extensive blood clotting, and abnormally low blood pressure.
- In short, the lives of each such patient would be imperiled. Just because the attackers modified small increments of data.

Fourth, what defenses of the target did the attackers force the target’s system to reveal? Attackers now have tools that can perform what’s known as an “execution run tracing and data falsification.” The tool forces a target’s system to “reveal secrets that are relied upon for security.” Directors, officers, and senior counsel may find this kind of tool easier to understand by noting that it works analogously to the flying of aircraft towards or extremely close to an adversary’s border (or even crossing it briefly and departing) in order to prompt the adversary to turn on its most sophisticated air defense radar, thereby revealing its location, signature, strength, and other features. In cyberattacks, as with

probing air defenses, the prospective attackers want to determine what actions will cause the defensive measures to be activated, or “turned on,” and when it counts, what actions will not cause the defensive measures to “turn on” and enable the attackers to bypass them. Not knowing what the attackers have learned may cause a target to be far more vulnerable to cyberattacks than the target (or an acquirer) may realize. It may also cause the target’s officers to become over-confident or complacent about their company’s cybersecurity.

Fifth, did the attackers gain entry by breaching a layer of the target’s system that did not have the same defenses as other layers? Many target companies are unaware of the fact that a protection system is only “reliably effective against attacks” that occur “at the same system layer in which the protection system” has been implemented – and that at some of a target’s computer network system layers there may be fewer or different protections than at others. As a result, the cyber attackers can breach a system by going through a layer that lacks protections at a higher or lower layer, just as attackers in medieval warfare could get past a deep moat and insurmountably high castle wall by tunneling beneath and past both of those defensive layers.

Thus a target’s exposure to cyber intrusions will be a function, in part, of how well prepared it is with tools to address those five features of a cyber incident.

For such reasons among others, the means for discovering vulnerabilities, closing gaps in defenses, detecting intrusions, figuring out what has been accessed, what has been done to it, and what awful things may happen at a time and place of the cyber intruder’s choosing, are the trailing-edge technologies. They lagged far behind the intruder’s technologies 20 years ago. Today they are even further behind. Methods of cyber intrusion, of conducting exploits, and of postponing their detection with stealth continue to outpace any improvements defenses. A victim’s first knowledge of an attack may come only when the damage or misuse of digital assets becomes conspicuous or reported by third parties. As a result, “companies often do not discover a data breach” or compromise of their digital assets “until an extended period of time after they have been hacked.”

4. Id.
2. Vulnerability of Target’s Digital Assets

A target of an acquisition should not be viewed as a safe repository of digital assets, nor as one that necessarily possesses assets the condition of which can be known with certitude. Given that the enterprise may be experiencing an ongoing cyber incident, the start of which may date back weeks, months, or years, the acquirer must consider the possibility that the security of the digital assets it seeks to buy can be described only in terms of indeterminate uncertainties.

Although the target’s high-value digital assets may appear intact, and customary descriptions of them make them seem secure, counsel should consider the possibility that such assets are (or have been) accessible to unauthorized third parties and have been altered or otherwise compromised. Thus, it is important to determine whether the target’s cybersecurity strategy (as reflected in its policies and procedures and its audits and incident reports) encompasses “avoiding asset loss and consequences; detecting asset loss and consequences; minimizing (i.e., limiting, containing, or restricting) asset loss and consequences; responding to asset loss and consequences; recovering from asset loss and consequences; and forecasting or predicting asset loss and consequences.”

Keeping sophisticated and well-resourced intruders out has become a formidable, if not impossible, task. As a NIST publication recently observed: “There is no system that can be engineered to be perfectly secure or absolutely trustworthy.”

Most companies’ high-value digital assets—such as intellectual property, business plans, operational and production data, and customer and employee information—are replicated in, stored on, and retrieved from digital media. Accordingly, acquirers should treat the target’s high-value digital assets as potentially cyber-vulnerable assets, i.e., cyber incidents could sharply reduce their value. Moreover, as measured by the scope and value of the assets, the risk and severity of cyber incidents have grown steadily. Major enterprises have tried, generally without success, to safeguard their high-value assets from cyber incidents and resulting compromise.

---

7. Id. at 16.
A compromise of digital assets occurs when an unauthorized person gains access to the assets with the ability to produce harmful results, such as:

- *exfiltrating copies of the assets* for any of a variety of harmful reasons, including public disclosure of confidential information (*e.g.*, to cause embarrassment), financial gain (*e.g.*, selling stolen trade secrets), reconnaissance (*e.g.*, gathering intelligence on the enterprise’s cybersecurity safeguards), or economic and industrial espionage (*e.g.*, learning an enterprise’s business plans, strategies, operational vulnerabilities, or causing reputational injury to persons or the enterprise);
- *altering, damaging, or destroying the digital assets*;
- *misusing the assets* to overcome system safeguards or to disrupt or damage a computer system; or
- *disabling, misdirecting, or otherwise sabotaging the assets’ performance* in order to disrupt or damage enterprise operations (*e.g.*, manufacturing processes, robotics managed assembly lines), especially those that a computer system is supposed to monitor and control with or without human intervention (*e.g.*, electricity generation, transmission, or distribution).

Nearly all companies have experienced compromises of their digital assets, regardless of whether they are aware of such compromises. Evidence of such compromises can be difficult to find and often appears only indirectly. Such evidence may include, for example: reports of breaches, the materiality of which was underestimated by the target’s IT staff or for whatever reason were not properly reported to senior management; reports of misuse of the target’s data from third-party suppliers, financial institutions, or other external sources; or evidence that the target has failed to take seriously the risk that its digital assets could be compromised and devalued by cyber incidents.

### 3. Vulnerability of Target’s Operations and Businesses

Cyber adversaries have become more selective of the enterprises they design their malware to attack. They now tend to launch targeted attacks. They have become more intent on damaging or disrupting their target’s operations and businesses, whether for personal gain, espionage, deliberate
sabotage, or political “hactivism.” The risks to enterprise operations are illustrated in a December 2014 report released by Germany’s Federal Office for Information Security that revealed cyber adversaries had attacked a steel mill in Germany by gaining access to the plant’s business network and then:

successively worked their way into production networks to access systems controlling plant equipment. . . . Once the attackers got a foothold on one system, they were able to explore the company’s networks, eventually compromising a ‘multitude’ of systems, including industrial components on the production network. ‘Failures accumulated in individual control components or entire systems.’ . . . As a result, the plant was ‘unable to shut down a blast furnace in a regulated manner’ which resulted in ‘massive damage to the system.8

Meanwhile, enterprises become inherently more vulnerable to cyber attacks with the adoption of new networked technologies, such as robots or other Internet-connected devices used in the manufacturing process:

As manufacturing systems become more complex and digitally connected, they become increasingly susceptible to disruptions that can cause significant financial losses. The U.S. Department of Homeland Security investigated 97 cyberattacks at critical manufacturers during the fiscal year ending in June 2015. . . . Cyberattacks to manufacturing plants are a relatively new phenomenon. The FY 2015 number that federal officials examined was double the previous year.9

To make matters worse, a target’s cybersecurity measures may not adequately address such risks to its operations and businesses or keep abreast

---

of the rapidly evolving threats. The target may also lack the resilience to withstand successful forms of such cyber attacks, which compounds the vulnerability of its operations and businesses (see the discussion of resilience in Chapter 10).

4. Vulnerability of Target’s Dependency on Critical Infrastructure

Cyber adversaries have become increasingly adept at exploiting the communication interlinkages among critical infrastructure sectors in order to launch attacks from a platform in one sector against enterprises in another sector. Deputy Treasury Secretary Sarah Bloom Raskin highlighted that development when she noted that attacks aimed initially at bulk electricity producers have been designed to cause disruption not only of the grid, but of the financial system: “We’ve seen attacks focused on power grids internationally. . . . If a power grid is taken out, that has an impact on the ability to clear payments.”

Cybersecurity often tends to focus on the direct impact a cyber attack may cause on an enterprise, but the collateral effect of an attack against another enterprise is also an important consideration. There are an increasing number of companies that have become “so critical to business productivity” that they are “systemically important” to an economic sector, a national economy, or the global economy. A cyber attack against one of those companies may indirectly, but adversely, affect another. For example, if a company critically depends on certain critical infrastructure suppliers (e.g., electricity or financial services), but has inadequate incident response and recovery plans to address the possibility that a cyber incident might disrupt the services of its critical infrastructure suppliers, that company’s ability to promptly restore its operations and business to preattack levels of service might be severely impeded.

Conversely, if “systemically important” companies do not understand their systemic importance and respond appropriately, their ability to


Chapter 2: The Importance of Cybersecurity Due Diligence for an M&A Deal

accelerate their recovery from a disruptive attack and mitigate the damage to their customers that rely upon them may be limited at best.

Although a few years ago large-scale, critical infrastructure risk scenarios would have been viewed as closer to science fiction than to reality, it is important to recognize that a large, multinational company or a mid-size regional supplier of critical infrastructure services will increasingly be exposed to such risks.

Moreover, if the cyber attack involves alteration of a company’s data with the aim of causing its personnel and customers to doubt the accuracy of the data on which they customarily depend, the resulting loss of situational awareness by the company and reduced trust in IT by business leaders, investors, and consumers (an “information malaise”\textsuperscript{12}) may be the most harmful consequence. In the aftermath, no one would know “which data is compromised and which is not.”\textsuperscript{13} Such scenarios appear to be an increasingly probable event, as the Cambridge Centre for Risk Studies emphasized:

> What is worrying is the potential for a global system-wide IT failure occurring across many organizations—a ‘correlated loss’ event that ultimately erodes value in a vast number of companies across multiple industries. As businesses become more globally interconnected, our research suggests this type of threat is increasing.\textsuperscript{14}

It would not be surprising to discover that most enterprises still rely on contracts containing boilerplate \textit{force majeure} and other risk management clauses that have not been updated to reflect the increase in cybersecurity risks or in the scale of consequences they can propagate.

5. Contamination of the Acquirer’s Networks and Data

An acquirer must be wary not only of failing to obtain the full value of what it seeks, but of belatedly finding the target to be burdened by cybersecurity deficiencies that create risks to the acquirer. An acquirer of a target’s digital assets and networks also acquires the cyber vulnerabilities of

\textsuperscript{12} Id.
\textsuperscript{13} Id. at 22.
\textsuperscript{14} Id.
the target’s digital assets and whatever malware the target may not realize has been injected into and could be operating on its networks and in its digital files. For example, malware may be currently in use by attackers within the target’s networks. Malware may have been secreted and designed to remain dormant until triggered to launch a later attack. Vulnerabilities may exist in the target’s networks and files that were exploited in earlier attacks without the target’s knowledge and could be exploited again in a future attack.

A target’s cybersecurity profile thus holds a dual key to a target’s disclosed risks: the potential devaluing of the target’s digital assets by cyber incidents, and the potential devaluing of the acquirer’s digital assets after it incorporates the target’s digital assets and networks into its own. These kinds of risks are unlikely to be identified and sufficiently assessed in a customary due diligence. A separate cybersecurity due diligence that focuses on identification and assessment of such risks may not find all of the sources of those risks in the target, but it can ensure they are investigated and improve significantly the chances of finding and illuminating them. It should also improve the acquirer’s comprehension of the risks the M&A deal may create when the acquirer’s and target’s respective digital assets (data, networks, and software programs) are integrated after the deal closes. As Safford’s rule puts it: “Sometimes the sum of the parts may be a ‘Hole’”15—i.e., the acquirer’s and targets systems, when interconnected, could lead to new vulnerabilities.

Each of the above-mentioned kinds of vulnerabilities has, to varying extents, appeared in recent cyber incidents, which are discussed in the next section.

6. Lessons from Recent Cyber Incidents

Recent cyber incidents involving iconic enterprises provide excellent examples of the critical importance of cybersecurity due diligence. Two incidents involved breaches of acquisition targets and compromises of their digital assets that we may infer were probably integral to the acquirer’s deal objectives:

- **Neiman Marcus**—where the cyber incident occurred during the acquisition, but was not discovered until after the closing when

it generated sizable incident expenses and potential liability to customers in class actions; and

- **Yahoo!**—where the two massive cyber incidents occurred years before the acquisition, one of which the target’s senior executives and legal department knew of but was not disclosed to the acquirer until months after the signing of the definitive Sale Transaction Agreements; at that point, the disclosed incident generated a demand by the acquirer that the target show the incident was not a “material” event. Eventually, the disclosed incident and discovery of a second incident led to a re-negotiation of the terms of the deal, including a $350 million reduction in the price.

Although we do not know the extent to which cybersecurity due diligence was done in these two transactions, they provide illuminating examples of the importance of a cybersecurity due diligence review. The Neiman Marcus incident illustrates the post-closing costs that the acquirer might have been better prepared to address had cybersecurity due diligence disclosed the ongoing compromise. The Yahoo! incidents show the problems resulting from a belated disclosure by a target of substantial compromises of its digital assets. Whether a cybersecurity due diligence was done, it is reasonably certain that the Yahoo! incident will inform the structure and use of cybersecurity due diligence in future acquisitions.

Three other incidents concerned companies not involved in an M&A transaction, but each incident involved the compromise of high-value digital assets that caused potentially significant reputational damage:

- **Target**—where the cyber incident compromised the company’s customer data and appeared, for some period of time, to diminish customer trust and its reputation as a trusted brand;
- **Sony**—where the cyber incident extensively damaged the computer resources of the enterprise, motivated the cancellation of a pending film release, and reduced the enterprise’s internal operations to analogue and paper communications; and
- **VW**—where the cyber incident originated inside VW and involved the company’s surreptitious introduction of “defeat-device” software into the engine emissions control systems of multiple makes and models of vehicles containing diesel engines in order “to cheat on federal emissions tests.”

cascade of costly fines and settlements that reduced the capital value of the company, devalued its brand, and dimmed its commercial prospects.

Any prospective acquirer would want the results of a cybersecurity due diligence review to identify a substantial compromise of the target’s high-value digital assets and to assess the impact it might have on the objectives of any ongoing M&A deal. Imagine negotiating and closing an acquisition of any of those companies without knowing: (i) of the cyber incident they experienced and the change it caused in the condition and value of its high-value digital assets; or (ii) whether the company’s response, if any, was effective or, instead, introduced new vulnerabilities that increased exposure of its digital assets to further cyber incidents and compromises.

These five incidents foreshadow the kinds of cyber incidents an acquirer, its counsel, and due diligence team should anticipate. They could happen to any enterprise. Such incidents thus illustrate the need for a cybersecurity due diligence review and may well justify and influence cybersecurity due diligence in future acquisitions.

For use in discussions with clients, we provide a brief account of the two incidents that affected M&A deals and of the three incidents that did not, but that offer cautionary lessons for an acquirer. Each account focuses on issues that an acquirer should have a firm grasp of when considering whether to direct a cybersecurity due diligence of a prospective target, when reviewing the reported findings, and when assessing the changes in terms and conditions it might seek in light of those findings.

6.1. Neiman Marcus

Luxury department store Neiman Marcus experienced, unawares, a cyber incident that began as early as July 16, 2013. The incident involved injection of malware into the retailer’s customer payment-processing system, potentially compromising data on about 350,000 customer payment cards.

Several weeks later, on September 8, 2013, as the intruders operated undetected within the retailer’s networks, Neiman Marcus agreed to be acquired by a group led by Ares Management and a Canadian pension plan. On October 25, 2013, the acquisition of Neiman Marcus closed. Five days later, on October 30, 2013, the card-scraping activity of the malware inside the retailer ceased. No report of the incident suggests that Neiman Marcus or its acquirers knew, as of the closing, that the digital assets of the retailer had been compromised by intruders.
On December 17, 2013, Neiman Marcus received the first of several reports indicating fraudulent use of customer credit cards at its stores. On January 10, 2014, Neiman Marcus publicly disclosed the incident. Shortly thereafter, affected customers filed class-action complaints alleging the retailer failed to protect them adequately against the breach and to provide them timely notice.

Although the district court dismissed the consolidated class-action complaint, holding that the plaintiffs had not shown they were at a substantial risk of harm and thus failed to meet Article III requirements for standing, the Seventh Circuit reversed. It concluded that

“[i]t is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach. Why else would hackers break into a store’s database and steal consumers’ private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers’ identities.”

In so holding, the Seventh Circuit pointed to the continuing risk, noting that: “stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.”

In March 2017, Neiman Marcus entered into a settlement with the class action plaintiffs and agreed to create a Settlement Fund in the amount of $1,600,000 to cover claims, legal fees, and other litigation related expenses.

18. Remijas v. Neiman Marcus Group, LLP, 794 F.3d 688, 693 (7th Cir. 2015).
19. Id. at 694 (quoting U.S. GOV’T ACCOUNTABILITY OFFICE, REPORT TO CONGRESSIONAL REQUESTERS: PERSONAL INFORMATION, GAO-07-737, at 29 (2007)).
Apparently, neither the buyer nor the seller knew that Neiman Marcus high-value digital assets had been compromised as of the closing, nor did they foresee the future risk of harmful use of such data. Lessons from the Neiman Marcus incident include:

• A stealthy cyber incident can proceed for months, compromise high-value digital assets, and cease without being discovered by the victim of the breach.
• Eventual discovery of a cyber incident may not occur until long after the closing of an acquisition.
• Given that the adverse consequences of a cyber breach may lie hidden for months or longer and then only be discovered from evidence of misused digital assets, it may be appropriate to revise the customary post-closing remedies that acquirers require to apply for a much longer post-closing period. In short, representations and warranties, covenants, and indemnifications might be modified to capture the cyber equivalent of “latent defects” and the potential impact of an incident’s long-delayed consequences.
• Acquirers might consider requiring a target to absorb a post-closing price adjustment for the costs of cyber incidents it should have discovered and disclosed, including serious incidents its IT personnel may have known of but failed to report to management and the board.
• Acquirers might also consider how to allocate the risk of losses caused by incidents too stealthy for the target to have been able to discover.
• Cybersecurity due diligence should be helpful in determining whether the target’s board properly understood the enterprise’s vulnerabilities, such as by requiring a comprehensive review of the company’s vulnerabilities: Does the target have the capabilities to detect intrusions? Can the target determine what changes the intruders may have made to the data? Or how they might be using copies of the data? And, does the target make a practice of reporting serious cyber incidents to management and the board?
• Cybersecurity due diligence may help an acquirer address the Neiman Marcus type of risks and uncertainties by revealing the extent to which the target’s cybersecurity program addressed the enterprise’s cyber vulnerabilities and its capabilities to detect intrusions, and whether its reporting of incidents to management and the board ensured they learn promptly of significant incidents.
• Cybersecurity due diligence can assist an acquirer in identifying deficiencies in a target’s safeguards, incident response procedures, and resilience (ability to withstand and recover from cyber incident repercussions). For example, Nieman Marcus reportedly disabled
Chapter 2: The Importance of Cybersecurity Due Diligence for an M&A Deal

...cybersecurity software (the function of which was to alert the company to “suspicious behavior”) and combined servers that in best practice should be segregated—namely, those that housed personal information and that housed financial information.21

As the Neiman Marcus incident illustrates, there is a growing need to assess a target’s cyber vulnerabilities and the potential repercussions from incidents so that they can be given their appropriate weight in the negotiations of a deal.

6.2. Yahoo!

In late 2014, senior officers and legal staff of Yahoo!, Inc., learned that unauthorized access to its computer network had been gained by what Yahoo! identified as a “state-sponsored actor.” Yahoo! did not, at that point in time, publicly disclose the incident. Yahoo!’s board apparently did not receive a report of the incident or learn of it until almost two years later.22

On July 23, 2016, Yahoo! and Verizon Communications Inc. (“Verizon”) entered into a stock purchase agreement by which Verizon agreed to acquire “one or more subsidiaries of Yahoo holding all of Yahoo’s operating businesses, for approximately $4.83 billion in cash ...”23 (hereafter referred to as the “acquisition of Yahoo!” or “Verizon/Yahoo! acquisition”). The acquisition of Yahoo! was “expected to close in the first quarter of 2017.”24

Around the same time as Yahoo! and Verizon signed their agreement, “a hacker claimed to have obtained certain Yahoo! user data. After investigating this claim . . . the Company could not substantiate the hacker’s claim. Following this investigation, the Company intensified an ongoing broader review of the Company’s network and data security, including a review of prior access to the Company’s network by a state-sponsored actor that the Company had identified in late 2014.”25

24 Id.
On September 22, 2016, Yahoo! publicly disclosed that a “copy of certain user account information for at least 500 million user accounts was stolen from Yahoo’s network in late 2014 (the First Security Incident).” Yahoo! disclosed the First Security Incident “13 days after the company issued a statement to the U.S. Securities and Exchange Commission (SEC) that said it had no knowledge of ‘any incidents’ of ‘security breaches, unauthorized access or unauthorized use’ of its IT systems.”26 After disclosing the incident, Yahoo! began notifying potentially affected users, regulators, and other stakeholders.

However, Yahoo! had commenced an investigation into the First Security Incident on July 30, 2016, five days after the deal “to sell Yahoo’s core business to Verizon . . . was struck.”27 For reasons that remain unclear, it took Yahoo! several weeks before it disclosed to Verizon that “at least some staff knew that a state-sponsored hacker had accessed its network shortly after an attack took place two years ago.”28

Media accounts report that Yahoo! disclosed the First Security Incident to Verizon only on September 20, 2016.29 A few weeks later, on October 13, 2016, Verizon’s general counsel told reporters during a roundtable discussion in Washington: “I think we [Verizon] have a reasonable basis to believe right now that the impact is material and we’re looking to Yahoo to demonstrate to us the full impact. If they believe that it’s not then they’ll need to show us that.”30 On the same day, Verizon’s chief financial officer reportedly stated, “we [Verizon] have a reasonable basis to believe right now that the impact [of the First Security Incident] is material.”31

In its November 9, 2016, Form 10-Q, Yahoo! disclosed:


27. Id.


An Independent Committee of the Board, advised by independent counsel and a forensic expert, is investigating, among other things, the scope of knowledge within the Company in 2014 and thereafter regarding this access, the [First] Security Incident, the extent to which certain users’ account information had been accessed, the Company’s security measures, and related incidents and issues.\textsuperscript{32}

Yahoo!’s 10-Q also disclosed that risks and uncertainties associated with the pending sale of Yahoo! to Verizon include “risks that Verizon may assert, or threaten to assert, rights or claims with respect to the Stock Purchase Agreement as a result of facts relating to the [First] Security Incident and may seek to terminate the Stock Purchase Agreement or renegotiate the terms of the Sale transaction on that basis[.].”\textsuperscript{33} The Verizon/Yahoo! acquisition agreement reportedly contained a clause that allowed Verizon to withdraw from the transaction if a new event “reasonably can be expected to have a material adverse effect on the business, assets, properties, results of operation or financial condition of the business.”\textsuperscript{34}

In the same 10-Q, Yahoo! made a disclosure concerning information it had received from law enforcement only two days before it filed the 10-Q:

Separately, on November 7, 2016, law enforcement authorities began sharing certain data that they indicated was provided by a hacker who claimed the information was Yahoo user account data. Yahoo will … analyze and investigate the hacker’s claim that the data is Yahoo user account data.\textsuperscript{35}

By November 9, 2016, when Yahoo! filed the 10-Q, “23 putative consumer class action lawsuits” had already been commenced against

\textsuperscript{32} Yahoo, Inc., supra note 23.
\textsuperscript{33} Id. at 69.
\textsuperscript{34} Id.
Yahoo! in U.S. federal and state courts and in foreign courts relating to the First Security Incident.\textsuperscript{36}

On December 14, 2016, five weeks after Yahoo! filed the Form 10-Q that addressed the First Security Incident, Yahoo! disclosed on its website and in a Form 8-K that the data provided by law enforcement (who received it from a hacker) appeared to be “Yahoo user data.” Analysis of that data by Yahoo!’s outside forensic experts convinced Yahoo! that a separate cyber incident had also occurred (the Second Security Incident): “[W]e believe an unauthorized third party, in August 2013, stole data associated with more than one billion user accounts. . . . We believe this incident is likely distinct from the incident we disclosed on September 22, 2016.”\textsuperscript{37} Yahoo! also disclosed a sophisticated contamination of data in its networks that involved the creation and use of “forged cookies” to access users’ accounts without a password and that involved the earlier attack by a state-sponsored actor.\textsuperscript{38} According to \textit{WIRED} magazine, the 2013 cyber incident was “the biggest known hack of user data ever, and it’s not really close.”\textsuperscript{39}

The \textit{Financial Times} reported on the immediate fallout: “A team of lawyers at Verizon are working to decide whether they can save the deal without exposing the US telecoms group to any future litigation linked to the data hack. . . . [U]nless Verizon was able to protect itself against future legal damages related to the data breach, it would be forced either to kill the deal or seek a discount on the transaction’s price.”\textsuperscript{40}

In January 2017, the SEC reportedly opened an investigation of Yahoo!, focusing on whether Yahoo!’s timing of its disclosures of the two breaches to investors complied with federal securities laws.\textsuperscript{41}

On February 1, 2017, in discussions between Verizon and Yahoo! on the “status of Verizon’s evaluation of the impact of the Security Incidents”

\textsuperscript{36} Id. at 42.
\textsuperscript{38} Id.
\textsuperscript{40} James Fontanella-Khan & Hannah Kuchler, \textit{Verizon’s $8.4bn Yahoo bid in doubt amid revelation over hack of 1bn users}, \textit{FIN. TIMES}, Dec. 16, 2016, at 1.
on Yahoo!’s business, Verizon indicated that the parties could “proceed in one of three ways.” The choices, as Verizon described them, demonstrated the extraordinary impact that the disclosure of the incidents was exerting on the parties’ re-negotiation of the terms of the acquisition:

(1) “Verizon could complete its evaluation of the impact of the Security Incidents on the [Yahoo!] Business over the next several months, after which Verizon would decide how to proceed and whether to assert any legal rights against Yahoo;”

(2) “Yahoo could agree to, among other things, a purchase price reduction in return for Verizon’s release of potential rights and claims in respect of the data security incidents;” or,

(3) “the parties could mutually agree to terminate the Sale Transaction [for Yahoo’s sale to Verizon].”^{42}

When asked by Yahoo! for the “magnitude of the purchase price reduction being requested by Verizon,” the reply was that “Verizon was still formulating a view but that a purchase price reduction as high as $925 million could be appropriate.”^{43}

On February 9, 2017, after further negotiations and as a result of the two cyber incidents, Yahoo! agreed with Verizon on the amount of the price reduction. On February 21, 2017, the parties agreed to modify the terms of the deal through Sale Transaction Agreement Amendments^{44} as follows:

• The purchase price was reduced by $350 million, down to $4.48 billion;
• Yahoo! would be responsible for all liabilities arising from shareholder lawsuits and SEC investigations related to the two cyber incidents;
• Yahoo! and Verizon would each be responsible for “50% of any cash liabilities incurred following the closing related to non-SEC … government investigations and third-party litigation related to the breaches.”^{45}

---


43. Id.

44. Id.

In addition to the $350 million reduction in the purchase price, Yahoo!’s 10-K, filed on March 1, 2017, disclosed further financial damages arising from the cyber incidents that would affect the parties to the transaction. Yahoo! disclosed it was “facing approximately 43 putative consumer class action lawsuits, four stockholder derivative actions and one putative stockholder class action … allegedly arising out of” the cyber incidents.46 Yahoo! recorded expenses of “$16 million” related to the cyber incidents in 2016, “of which $5 million was associated with the ongoing forensic investigation and remediation activities and $11 million was associated with nonrecurring legal costs.”

Yahoo!’s 10-K also disclosed the findings of the independent committee of its Board of Directors that had been investigating the First Security Incident and what was known about it in 2014 that had not been reported to the Board until after Yahoo! and Verizon signed the Stock Purchase Agreement. Unlike the cyber intrusions at Neiman Marcus which went undetected for months, Yahoo!’s information security team detected the First Security Incident the same year (although the 10-Q omits disclosing how many weeks or months passed between the start of the intrusion and its detection by Yahoo!):

“The Independent Committee [of the Board] concluded that the Company’s information security team had contemporaneous knowledge of the 2014 compromise …”47

Most importantly, the Independent Committee of the Board found that senior executives and legal staff also had such knowledge in 2014, yet did not report the First Security Incident to the Board. The 10-Q does not give any reasons for the disconnect between possessing knowledge of such ominous significance and not sharing it with the Board. The 10-Q limits its disclosure to who knew what and when and what they failed to do:

“In late 2014, senior executives and relevant legal staff were aware that a state-sponsored actor had accessed certain user accounts … While … security measures were implemented in response …, it appears certain

47. Id. at p. 47. [Emphasis added.]
senior executives did not properly comprehend or investigate, and therefore failed to act sufficiently upon, the full extent of knowledge known by the Company’s information security team.”

Although the Independent Committee of the Board “did not conclude that there was an intentional suppression of relevant information,” it nonetheless found that the

“relevant legal team had sufficient information to warrant substantial further inquiry in 2014, and they did not sufficiently pursue it. As a result, the 2014 Security Incident was not properly investigated and analyzed at the time, and the Company was not adequately advised with respect to the legal and business risks associated with the 2014 Security Incident. … [T]he Audit and Finance Committee and the full Board were not adequately informed of the full severity, risks, and potential impacts of the 2014 Security Incident …”

In response to the Independent Committee’s findings, Yahoo!’s Board made decisions concerning the CEO and GC:

- It determined not to award the CEO a cash bonus for 2016 “that was otherwise expected to be paid to her;”
- It accepted the CEO’s offer to “forgo any 2017 annual equity award given that the 2014 Security Incident occurred during her tenure;” and,
- Upon the resignation on March 1, 2017, of the GC, no payments were made to him “in connection with his resignation.”

In mid-March 2017, the U.S. Department of Justice indicted two Russian Federal Security Service (“FSB”) officers and two others

“for computer hacking, economic espionage and other criminal offenses in connection with a conspiracy,

48. Id.
49. Id.
50. Id.
Beginning in January 2014, to access Yahoo’s network and the contents of webmail accounts.”

Lessons from the Yahoo! cyber incident include:

- Since Yahoo!’s security team, senior executives, and legal staff knew of the cyber incident in 2014, and Yahoo!’s Board did not learn of it until at least mid-2016 or later, it appears that there was a breakdown in Yahoo!’s incident response procedures or those procedures were not designed to address serious cyber incidents.

- Cybersecurity due diligence teams should, therefore, not assume that a target’s security team, senior officers, and legal staff will necessarily report to their board when they learn that their company has experienced a potentially damaging cyber incident. They are capable of underestimating an incident’s significance and of failing to act to protect the enterprise. That may happen even when they know, or should know, that the intruders could extend their attack deep into the enterprise, that the intruders are state-sponsored actors, and the company’s high-value digital assets are at extreme risk for as long as the intruders continue to operate within the enterprise’s networks.

- Cybersecurity due diligence teams may, therefore, need to consider the possibility that failures of the kind that occurred in Yahoo!’s incident response procedures could happen at any company, and that they may need to closely examine the evidence of previous incidents at the target in order to assess whether reporting channels from the security team up the chain of command to the C-suite officers and the Board are, in fact, reliable, and if not, what enhanced due diligence may be needed to gain an accurate view of the target’s previous and current experience of cyber incidents.

- Given that Verizon only learned of the First Security Incident when Yahoo! disclosed it in late September 2016, it appears that Verizon’s due diligence team had not, by that date, discovered any record of the incidents from late 2014 and from July 2016. Cybersecurity due diligence teams may need to be wary of relying on a target’s descriptions of its experience of cyber incidents, especially if the target is iconic, of probable interest to state-sponsored hackers, and

acknowledges such a small number of cyber incidents as to raise concerns that it is “too few to be true.” In that event, the target may not know what it should know of its cyber incidents, or there may be breakdowns in reporting serious incidents to the C-suite officers and the Board or in disclosing them to the due diligence team.

- Given that Yahoo! appears to have received potentially credible evidence of the First Security Incident in July 2016, there may be a question as to whether due diligence could have discovered that Yahoo! had “intensified an ongoing broader review of the Company’s network and data security, including a review of prior access to the Company’s network by a state-sponsored actor that the Company had identified in late 2014.”

- Although cybersecurity due diligence should not be expected to discover ongoing, stealthy, cyber incidents, it should be capable of discovering evidence of earlier known incidents, breakdowns in cyber incident reporting, and undisclosed internal investigations of security by the target before and during an acquisition.

- A target’s Board might be unaware of their company’s recent experience of serious cyber incidents, notwithstanding the prodigious size of the company and its reputation for expertise in digital and Internet businesses.

- Both Yahoo! and Neiman Marcus demonstrate the need to consider adjusting the conceptual time frames counsel uses in acquisitions. Although the state-sponsored intrusion of Yahoo! was first discovered in late 2014, it may have begun months or years earlier. Thus, a cybersecurity due diligence team may need to examine cybersecurity-related records and information dating back several years.

- Similarly, the fact that Yahoo!’s Board did not learn of the First Security Incident for over two years, and that Yahoo! belatedly disclosed the Incident to Verizon, suggests that cybersecurity due diligence should include an early and rigorous round of interviews to create a baseline about what is known (and becoming known) of cyber incidents by the target’s security team, senior officers, and legal staff.


6.3. Target Corporation

On December 19, 2013, the Target Corporation (Target Corp) disclosed that it had experienced a breach of its networks affecting 40 million credit- and debit-card numbers and personal identifiable information for up to 70 million individuals. The company’s 10-K for the fiscal year ending February 1, 2014, treated the incident as “material” individually and provided a description of the cyber incident:

In the fourth quarter of 2013, we experienced a data breach in which an intruder stole certain payment card and other guest information from our network (the Data Breach). . . . [T]he intruder accessed and stole payment card data from approximately 40 million credit and debit card accounts of guests who shopped at our U.S. stores between November 27 and December 15, 2013, through malware installed on our point-of-sale system. . . . In addition, the intruder stole certain guest information, including names, mailing addresses, phone numbers or email addresses, for up to 70 million individuals.54

The 10-K detailed the incident’s costs and consequences through the fourth quarter of 2013:

- “$61 million of pretax Data Breach-related expenses, and expected insurance proceeds of $44 million, for net expenses of $17 million ($11 million after tax), or $0.02 per diluted share. . . . We believe that it is reasonably possible that the ultimate amount paid on payment card network claims could be material to our results of operations in future periods.”55
- “The Data Breach . . . negatively impacted our ability to timely handle customer inquiries, and we experienced weaker than expected U.S. Segment sales following the announcement of the Data Breach.”56
- “[M]ore than 80 actions have been filed in courts in many states and other claims have been or may be asserted against us on behalf of

55. Id. at 48–49.
56. Id. at 9.
guests, payment card issuing banks, shareholders or others seeking damages or other related relief arising out of the Data Breach. . . .”

- Target Corp’s profits in the fourth quarter of 2013 dropped 46 percent compared with the year before.

In its subsequent 10-K for the fiscal year ending January 31, 2015, Target Corp reported that it had “incurred $252 million of cumulative Data Breach-related expenses, partially offset by $90 million of expected insurance recoveries, for net cumulative expenses of $162 million.”

The data breach also prompted Target Corp to incur security improvement costs. As it explained in a 2014 press release, the company decided to accelerate its “transition to chip-and-PIN-enabled REDcards” and, thereby, incur $100 million to upgrade its cybersecurity.

Significantly, the largest potential damages identified by Target Corp were to its reputation and customer trust. If customers cannot make purchases without fear of having their payment card data stolen, they may shop elsewhere. As the company explained in its 2013 10-K: “[W]e believe that the greatest risk to our business arising out of the Data Breach is the negative impact on our reputation and loss of confidence of our guests. . . .”

### 6.4. Sony Pictures

On November 24, 2014, North Korea launched (via servers in Taiwan) a cyber attack against Sony Pictures Entertainment that injected hard-drive erasing malware into the company’s networks. By wiping the hard drives, the attack ruined more than 3,000 computers and 800 servers and destroyed the copies of data stored within them.

To continue operations, at a sharply reduced level, Sony interrupted its reliance on digital communications and reverted to predigital operations. It shut off all connections with the Internet, to the rest of Sony, and to

---

57. Id. at 7.


61. TARGET CORP., supra note 59, at 13.
third parties. During its recovery, Sony’s only communications with the outside world were via “landline telephones and hand-delivered messages written with pen and paper.”

62 Damages to Sony were estimated at about $100 million, in comparison to the $171 million Sony estimated it incurred as a result of the cyber incident involving its Playstation Network in 2011 (a more costly incident due to the compromise of customer data). 63

6.5. Volkswagen

The cyber incident at Volkswagen, that came to be known as “dieselgate,” depleted trust in the enterprise, damaged the credibility of its officers’ statements to regulators and customers, and devalued the corporate brand. 64 Here, no outside hacker designed and exploited an attack on VW’s vehicles. Insiders apparently conceived, planned, and executed a surreptitious alteration of the company’s software that controls vehicle onboard systems. The purpose: to make it appear in emissions control tests that VW’s diesel vehicles met U.S. and California emission-control limits when, in fact, they exceeded them by up to 40 percent. The company crafted the defeat-device software that gave its vehicles the false appearance of compliance. It concealed the activity for years. When regulators asked whether VW had modified its engine and emissions control software, VW continued the concealment, issuing on behalf of the company a succession of disingenuous denials. 65

The VW defeat-device software does not appear to have affected an M&A deal, but is discussed here because activities such as this are relevant to such deals. A prospective acquirer of VW, or of any company that has

62. 60 Minutes: The Attack on Sony (CBS television broadcast Apr. 12, 2015).
64. Acknowledging the depletion trust, VW CEO Matthias Mueller told an annual financial conference in Wolfsburg, Germany in April 2016, “We know that we have disappointed many people—people who have placed their trust in Volkswagen. . . . And we are doing everything in our power to regain trust.” Jessica Hartogs, VW CEO says priority is to ‘regain trust’ after emissions scandal, CNBC, Apr. 28, 2016, http://www.cnbc.com/2016/04/28/vw-ceo-says-priority-is-to-regain-trust-after-emissions-scandal.html.
inappropriately and surreptitiously modified its own products to deceive regulators and the public, would want to know of such activity and the risks of successor liability when the misdeeds came to light.

From August 2008 through September 2015, VW installed the defeat-device software in multiple makes and models of its diesel vehicles—eventually 11.5 million autos worldwide. The software enabled a vehicle’s emission system to detect driving characteristics indicative of operations under test-lab protocols (e.g., straight-line acceleration, fixed position of steering wheel) and indicative of highway operations.

- Detection of test-lab operations activated the vehicle’s emission control system and suppressed emissions of nitrous oxide (NOx) to levels compliant with U.S. and California standards. It also limited the vehicles acceleration and its fuel economy.
- Detection of highway operations deactivated the vehicle’s emission control system and allowed the vehicle to generate enhanced acceleration, achieve fuel economy, and exceed by a factor of up to 35 the legal limit for NOx emissions.

The defeat-device software thus avoided the downside of an engineering tradeoff: emissions control compliance forced other automotive manufacturers to cut acceleration and fuel economy. VW’s software disguised its avoidance of that tradeoff and created the appearance of compliance with environmental protection laws in the test labs while circumventing them on the highway.

The stealth of VW’s hack of its engine emission control systems concealed the ongoing cyber incident for over seven years. VW gained the final year-and-a-half of concealment by issuing disingenuous denials when U.S. and California regulators questioned VW about the discrepancies between test lab and highway emissions of its diesel vehicles. VW admitted to the installation of defeat-device software only when U.S. regulators threatened to withhold issuing VW the requisite certificates for import of its 2016 diesel models.

VW eventually pled guilty to having engaged in criminal conduct and admitted that from “approximately May 2006 to approximately November 2015, VWAG . . . agreed to deceive U.S. regulators and U.S. customers about

whether” certain of its vehicles complied with U.S. emissions standards. VW knew that its vehicles “did not meet U.S. emissions standards,” that “VW was using software to cheat the U.S. testing process by making it appear” as if its vehicles “met U.S. emissions standards when, in fact, they did not,” and “attempted to and did conceal these facts from U.S. regulators and U.S. customers.”

VW’s exposure to damages from the cyber incidents that consisted of its writing and installing the defeat-device software have included:

- a court-approved $14.7 billion settlement with owners of 475,000 VW diesel-powered vehicles with two-liter engines and government agencies;69
- a court-approved plea agreement with the U.S. Department of Justice in which VW pled guilty to three criminal counts: (i) “conspiracy in violation of 18 U.S.C. § 371”; (ii) “obstruction of justice in violation of 18 U.S.C. § 1512(c)”; and (iii) “introducing imported merchandise into the United States by means of false statements in violation of 18 U.S.C. § 542,” and VW agreed to pay a fine of $4.3 billion;70
- a court-approved settlement with owners in Canada of 105,000 VW diesel-powered vehicles with two-liter engines to pay up to C$2.1 billion (U.S.$1.6 billion) to buy back or fix the vehicles, an amount that includes a civil fine of C$15 million;72
- a court-approved $1 billion settlement with owners of 83,000 VW diesel-powered vehicles with three-liter engines and with government agencies;73

• agreement to pay approximately $1.2 billion to its 652 U.S. dealers as compensation (an average of $1.85 million per dealer); 74
• a settlement, pending court approval, to pay $1.2 billion to about 75,000 U.S. owners of three-liter, diesel-powered vehicles and offering proposed fixes to other owners; but if U.S. regulators do not approve the proposed fix for such cars, VW will be “forced to buy them back, increasing the cost of the settlement . . . to more than $4 billion”; 75
• suits filed by the attorney generals of New York, Massachusetts, and Maryland alleging the company made false statements to regulators and violated environmental protection laws and claiming (in the case of New York) state penalties of over $500 million; 76
• an investor’s lawsuit in the Braunschweig district court in Germany seeking about $9.1 billion in damages on losses suffered when VW’s shares plunged after public disclosure that the company had circumvented and cheated emissions tests; 77 and
• “[o]perating profit at the Volkswagen passenger car unit . . . down more than 45 percent . . . for the first nine months of 2016. . .”; 78

The costs of “dieselgate” had thus risen to at least $22.4 billion and possibly in excess of $25 billion by February 2017, 17 months after VW’s public disclosure of the use of defeat-device software. 79 Damage to VW’s brand and credibility is hard to quantify, if not inestimable; however, it appears that each has steeply declined as evidenced by the conspicuous irony that has attached to the motto of VW’s Audi

78. McGee, supra note 76, at 1.
brand “Truth in Engineering” and to the slogan of VW’s brand in North America “Isn’t it time for German engineering?”

Lessons from Target Corp, Sony, and VW include the following:

- Cybersecurity due diligence should enable an acquirer to discover where a target has allowed its practices to become noncompliant with its security policies and to highlight those as potentially significant cyber vulnerabilities of digital assets.

- As the Sony incident demonstrates, cybersecurity due diligence should consider whether a target has included in its worst-case-scenario incident planning the possibility that it or its critical infrastructure suppliers will experience a kinetic, cyber incident that destroys its computers, networks, and on-site copies of digital data.

- VW’s development and deployment of defeat-device software reveals a new and significant insider threat—the design and use of “corrupt software”—that can be secreted within a target and that cybersecurity due diligence should ideally be designed to detect.


81. Commentators have begun to characterize the VW’s defeat-device software as an insider cyber threat:

> Usually, we think of cybersecurity in terms of protecting software from external attacks. But the Volkswagen emissions scandal is a reminder that software integrity can also be intentionally compromised from the inside. This isn’t a classic ‘cybersecurity’ problem since the deceptive software works exactly as designed. But it is certainly a problem of cyber trust. . . .

> Consider, for example, a maker of home appliances that wanted to boost sales by shipping refrigerators with software designed to cause premature failure. . . . [And] suppose that the manufacturer was . . . clever, designing the software to cause most (but not all) of its refrigerators to fail on a randomly chosen date between seven and ten years after purchase. This self-inflicted cyber-sabotage would significantly shorten the average replacement time, leading to higher future sales for the manufacturer.

• Cybersecurity due diligence should alert an acquirer to compromising activities by the target that may put not only its digital assets, but its customer trust and brand loyalty at risk.

• The cyber vulnerability of a target’s digital assets will be heightened where such assets are constituent components of new and widely deployed technologies that bring with them a proliferation of cyber vulnerabilities:

  [P]eople routinely put trust in machines and the people who create them. Software involves perhaps the greatest trust of all. It’s the most malleable, most complex, and least visible of engineering artifacts. Future developments like the Internet of Things and robotics can only magnify this trend. Consider the trust implicit in riding a self-driving car or in a walking robot carrying a person with a disability.  

Omitting cybersecurity assessments in M&A due diligence, conducting superficial evaluations, or limiting such due diligence to a company’s IT systems rather than treating cybersecurity as a risk category in its own right means ignoring the serious risks that cyber threats pose to all companies and to M&A deals involving them.

82. Trope & Ressler, supra note 65, at 28.