ALTEN TECHNOLOGY

FIVE KEY BENEFITS OF INVESTING IN CYBERSECURITY

by
Eric Nyberg and Rachel Sellers

5 May 2024

ALTEN

INTRODUCTION

Over the last five to ten years, individual consumers have shared more and more personal data with companies online. In 2017, just one in five interactions between consumers and companies took place online. By 2020, the percentage had skyrocketed to more than 50 percent.[1]

In most cases, consumers must share personal data to gain the benefits provided by companies online, so consumers trust that companies will protect this shared data. To provide the necessary level of security, companies must hire cybersecurity experts. With the promise of increased efficiency and productivity, why would advancements in IT be deemed a risk and cause for concern? The answer: cybercrime.

As businesses collect more data and increasingly rely on their digital infrastructure—and cyberattacks of all kinds become more frequent, sophisticated, and damaging—investing in cybersecurity is more critical than ever. According to the Verizon Data Breach Investigation Report, the number of data breaches around the world more than tripled between 2013 and 2021.[2] Even companies with strong security practices are at risk. More than 60 percent of the 1,000 largest US companies have experienced public data breaches, and the Cyentia Institute estimates that one in four companies will experience a corporate breach annually,[3] claiming that "there's a six percent chance that a Fortune 1000 firm will lose $100 million or more in a 12-month period due to cyber events."[4]

In addition to helping companies avoid the costs associated with a cyberattack, investing in cybersecurity brings a host of other benefits, including being prepared to effectively respond to cybersecurity incidents, mitigating risks as technologies and threats evolve, ensuring data security and availability, gaining a competitive advantage, and complying with regulatory requirements. Together, these benefits protect a company's financial future and its reputation with B2B customers and consumers.

AVOIDING THE GROWING COSTS OF CYBERATTACKS

One of the obvious benefits of investing in cybersecurity is avoiding losses associated with a cybersecurity incident, including monetary losses, decreases in share prices, downtime, and damage to the company's brand reputation. According to annual reports released by the FBI's cybercrime department, the Internet Crime Complaint Center (IC3), the estimated losses caused by cybercrime have steadily increased in the recent years, rising from $4.2 billion in 2020[5] to $6.9 billion in 2021[6] and $10.3 billion in 2022.[7] In a span of ten years (2013–2023), the annual amount of monetary damage caused by reported cybercrime in the United States has increased more than tenfold.[8]

The damage a cyberattack can cause to a company isn't only monetary. A great example of the far-reaching effects of a cyberattack can be seen in the 2020 SolarWinds supply chain hack, which is still affecting SolarWinds and having a significant impact on security measures around the globe. SolarWinds specializes in developing software for network, system, and IT infrastructure management. In 2019, state-sponsored hackers compromised Orion, SolarWinds' flagship network monitoring software, and then used a tainted update in March 2020 to gain access to the systems of up to 18,000 of SolarWinds' customers, including nuclear laboratories, Fortune 500 corporations, and several government bodies.[10] SolarWinds' stock value plummeted by 25 percent within two days of notifying shareholders and customers of the attack,[11] and by month's end it had declined 40 percent overall.[12] The immediate financial cost of the breach exceeded $40 million, but the potential damage to SolarWinds' reputation is incalculable.[13] In late 2021, a class action lawsuit filed against SolarWinds resulted in a $26 million settlement,[14] and in October 2022, the US Security and Exchange Commission (SEC) informed SolarWinds that it would be conducting an investigation "with respect to its cybersecurity disclosures and public statements, as well as its internal controls and disclosure controls and procedures."[15]

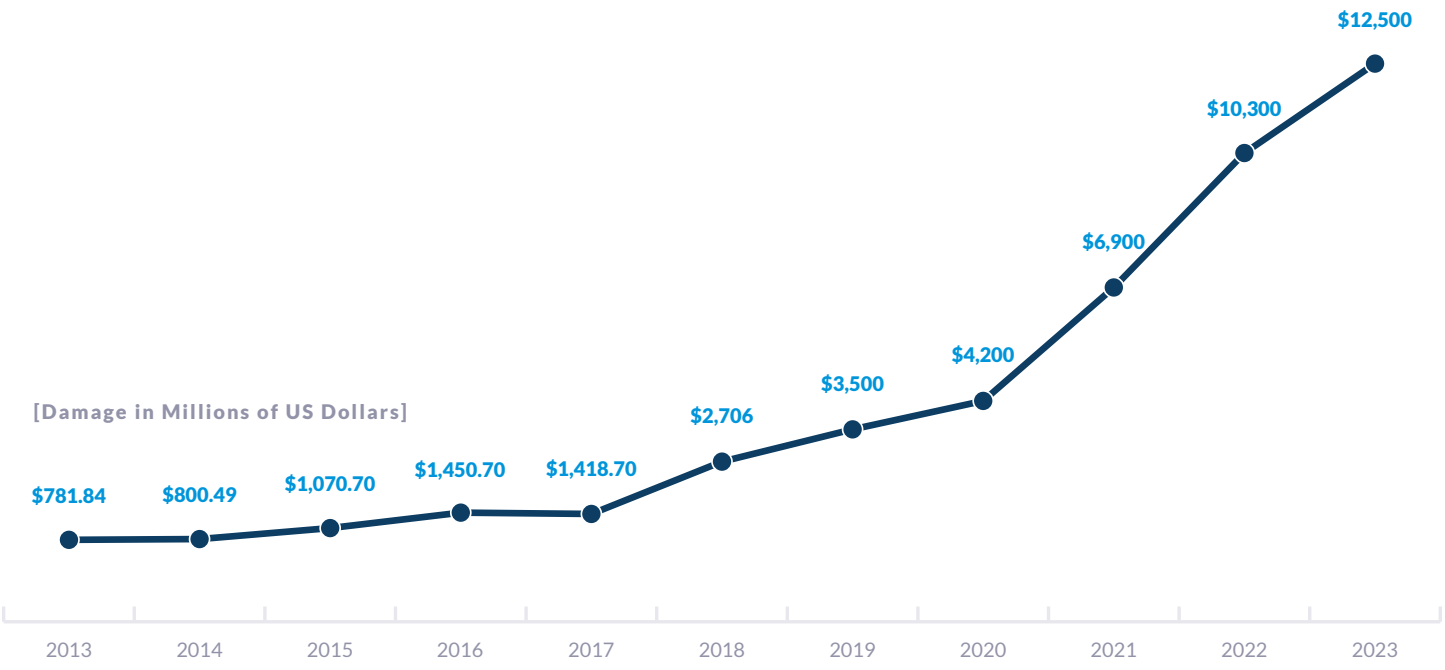

FIGURE 1. ANNUAL AMOUNT OF MONETARY DAMAGE CAUSED BY CYBERCRIME REPORTED TO THE IC3 IN THE UNITED STATES FROM 2013 TO 2023[9]

BEING PREPARED TO EFFECTIVELY RESPOND TO A CYBERSECURITY INCIDENT

Although robust cybersecurity is key to preventing cyberattacks, cybersecurity is always engaged in an arms race between would-be attackers and security personnel. When a cyberattack is successful, an effective response can make the difference between a company shutting down its operations, losing revenue, and suffering damage to its brand reputation versus being able to effectively operate during an attack, repel assailants, and successfully recover.

Companies vary in their approaches to handling data breaches and cyberattacks. However, the most effective way for a company to regain trust, recover its reputation, and comply with US federal regulations is by openly addressing cyber incidents. As of December 18, 2023, publicly traded companies must comply with new SEC incident disclosure regulations, which require that companies report material cyber incidents within four business days.[16]

The actions taken by Norsk Hydro, a Norwegian renewable energy and aluminum manufacturing company, are a notable example of an effective response to a ransomware attack. When Norsk Hydro realized it was under attack in March 2019, it shut down all its systems and refused to pay the ransom demanded by its attackers,[17] a best practice recommended by cybersecurity experts, including the US FBI.[18] During the attack, Norsk Hydro maintained a level of operation by reverting to a paper-based process and controlling all of its equipment manually, which allowed it to fulfill simple orders while it rooted out the attackers in a months-long recovery process. It enlisted the help of Microsoft's cybersecurity response team and the Norwegian National Cyber Security Centre in its recovery efforts, creating teams to investigate the virus, inspect business operations, and rebuild the network from trusted backups. Norsk Hydro was highly transparent about the attack and its recovery efforts in the following months. Security experts praised this welcome departure from the secretive responses companies typically give in the wake of an attack.

> When a cyberattack is successful, an effective response can make the difference between a company shutting down its operations, losing revenue, and suffering damage to its brand reputation versus being able to effectively operate during an attack, repel assailants, and successfully recover.

Despite these efforts, the ransomware attack inflicted substantial financial losses on Norsk Hydro. The company estimated the total cost of the incident to be over $71 million, including expenses related to recovery efforts, lost production, and reputational damage. However, thanks to the company's responsiveness and preparedness, this is undoubtedly lower than the cost might have been if the company been less prepared and handled the incident differently. Norsk Hydro has since implemented robust cybersecurity procedures to reduce the likelihood of future attacks.[19, 20]

ENSURING DATA AVAILABILITY, RELIABILITY, AND SECURITY

Having strategies to ensure that data is available, reliable, and secure is vital for any company's operational excellence and financial well-being. Properly protecting a company's sensitive information regarding itself, its customers, and its processes reduces the risk of unauthorized access and data breaches, as well as the accompanying regulatory fines and legal repercussions. By maintaining data integrity and confidentiality, a company bolsters its customers' trust and its own reliability, creating a solid foundation for loyalty and long-lasting relationships. Ensuring efficient data availability also allows employees to reliably access critical data when needed, which increases productivity and promotes better decision-making for management. The bottom line is that data is a valuable asset, and it pays to protect it and ensure that it's accessible to those who need it.

Two incidents illustrate the value of data and the financial losses that a period of unavailability can bring, regardless of the cause. In 2017, Amazon Web Services (AWS) experienced a four-hour outage caused by human error during maintenance. This outage removed a larger set of servers from the system than intended and took down a large number of websites hosted on AWS, including websites for publishers, S&P 500 companies, and US financial service companies.[21] According to news website Axios, economic modeling startup Cyence estimates that this outage led to between $150 and $160 million worth of losses for the affected S&P 500 and financial services companies.[22] In the second incident, a system failure resulting from a power supply issue caused a 2017 British Airways outage, leaving 75,000 customers stranded over a holiday weekend. The outage caused the stock of British Airways' parent company, IAG, to drop, resulting in a £170 million loss in value. The outage also led to British Airways paying more than £100 million in compensation for the unavailable systems.

MITIGATING RISKS AS TECHNOLOGIES AND THREATS EVOLVE

> Prioritizing cybersecurity in any critical infrastructure is vital to mitigating external threats, maintaining the integrity of processes, and ensuring confidence in critical infrastructure security.

In addition to protecting against cyberattacks and other cyber threats, investing in robust cybersecurity practices and establishing an infrastructure with strong security measures enables businesses to more easily incorporate new technologies into their business model without inadvertently introducing potential risks.

Imagine a scenario in an operational technology (OT) environment where you seek to optimize your manufacturing processes by introducing a new feature into your industrial control system (ICS). Realizing that there is a need for predictive maintenance to optimize your business, you decide to implement a sensor-based monitoring system to gather real-time data on equipment performance. This data is processed and stored in your ICS for analysis and managed via a supervisory control and data acquisition (SCADA) system to enhance the overall efficiency of your OT environment. This new system enables maintenance teams to monitor equipment performance from remote locations. However, this improvement inadvertently introduces a cybersecurity vulnerability. Remote access, although convenient for monitoring and efficiency, creates a potential entry point

for unauthorized users to manipulate the sensor data or even gain control over critical industrial processes.

This scenario highlights the vital importance of implementing strict cybersecurity measures from the first design phase for any OT system improvement. Without proper security measures such as strong authentication protocols, encryption methods, and regular security audits, your industrial processes may be susceptible to unauthorized remote manipulation. Had adequate cybersecurity design processes been in place from the beginning, the company could have proactively addressed this vulnerability, preventing potential disruptions and ensuring the reliability of manufacturing operations. Prioritizing cybersecurity in any critical infrastructure is vital to mitigating external threats, maintaining the integrity of processes, and ensuring confidence in critical infrastructure security.

Now consider an automotive OEM. The OEM is constantly trying to achieve operational excellence, reliability, cost-effectiveness, and availability for its business as well as for its vehicles. As technology and the potential for connectivity have advanced, so too have vehicles and the vehicle industry. The OEM's vehicles are no exception to this trend, and its vehicles are connected and capable of receiving signals, data, and input from outside sources. The vehicle will thus have potential security risks and may be vulnerable to outside manipulation.

This vulnerability proved to be all too real in 2015, when two security researchers demonstrated their ability to remotely take control of a Jeep Cherokee as it was driving 70 mph down a highway. The researchers successfully hacked the vehicle through the cellular connection of the car's entertainment system, then rewrote the firmware in the vehicle's head unit, allowing the researchers to take absolute control of the vehicle's steering, transmission, brakes, and even the engine, all while the volunteer driver was unable to do anything but watch helplessly. Cybersecurity risks turn into potentially life-threatening risks when hackers don't have to be anywhere near a car to intercept signals and take control of the vehicle.[24]

PROVIDING A COMPETITIVE ADVANTAGE TODAY AND FACILITATING REGULATORY COMPLIANCE TOMORROW

Companies are becoming more aware of the need for a strong cybersecurity posture to protect against evolving threats, leading them to work with other businesses with good cybersecurity practices. In an increasingly interdependent business landscape, where one weak link in the supply chain can have remarkable and far-reaching consequences (just look at SolarWinds), it pays to be able to demonstrate to your partners and stakeholders that you aren't a potential liability. Well-established security processes, policies, and capabilities may give you an edge in competitive bids, especially if your company is certified to standards like ISO 27001.

The earlier a company implements and partners with other companies that are certified to ISO 27001 and other critical cybersecurity standard practices, the better off it will be. By implementing strong, robust design practices early in the development, you'll ensure your code is not full of potentially exploitable weaknesses that will only be harder to identify and fix as you grow and your code gets more complex.

In an increasingly interdependent business landscape, where one weak link in the supply chain can have remarkable and far-reaching consequences (just look at SolarWinds), it pays to be able to demonstrate to your partners and stakeholders that you aren't a potential liability.

Robust cybersecurity practices don't just give companies a leg up on competitors, however; they are increasingly necessary for doing business at all. The automotive industry is an example of this trend of increasing cybersecurity regulation. In 2016, the US National Highway and Traffic Safety Administration (NHTSA) released the first edition of its *Cybersecurity Best Practices for the Safety of Modern Vehicles*.[25] Although this document contains "nonbinding guidance to the automotive industry for improving vehicle cybersecurity," subsequent updates in 2020[26] and 2022 incorporated practices outlined by ISO/SAE 21434:2021[27] that harmonize with the United Nations Economic Commission for Europe (UNECE) WP.29 Cybersecurity Regulation R155.[28] Unlike the NHTSA guidance, UNECE Cybersecurity Regulation R155 and its accompanying regulation R156 are binding regulations passed by UNECE in June 2020 that require vehicle manufacturers to take action in several areas:

- Managing vehicle cyber risks;
- Securing vehicles by design to mitigate risks along the value chain;
- Detecting and responding to security incidents across vehicle fleet;
- Providing safe and secure software updates and ensuring vehicle safety is not compromised, introducing a legal basis for so-called "over-the-air" (OTA) updates to on-board vehicle software.[29]

The regulations apply to passenger cars, vans, trucks, and buses. In the EU, compliance has been mandatory for all new vehicle type approvals since July 2022 and is mandatory for all new vehicles produced from July 2024.[30] Although the UNECE regulations aren't binding in the US, it is likely that cars sold in the US will still be built to meet these cybersecurity standards. As a GM spokesperson told the *New York Times*, "The UN regulation is a global standard, and we have to meet global standards."[31]

CONCLUSION

Investing in cybersecurity has never been more important, thanks to the growing collection of consumer data; greater business reliance on digital technology; and increasingly sophisticated, frequent, and damaging cyberattacks. In addition to helping businesses avoid the potentially enormous financial and reputational costs of a cyberattack, investing in cybersecurity has several benefits, ranging from being prepared to effectively respond to a cyberattack to facilitating future regulatory compliance, and ultimately protecting a company's reputation.

Facilitating continuity, resilience, efficiency, and customer and partner relationships while mitigating financial risks, data breaches, and downtime is essential for any business's success. Although internal cybersecurity personnel and resources are critical investments, navigating the best way to implement cybersecurity technologies, processes, and procedures can be complex and difficult for businesses looking to improve their cybersecurity. Partnering with expert cybersecurity consultants like ALTEN Technology can help businesses quickly maximize the potential benefits of cybersecurity without getting lost in the ever-changing cybersecurity landscape.

SOURCES

1. Madnick, Stuart E., "The Rising Threat to Consumer Data in the Cloud," *Apple*, December 2022.
2. Data Breach Investigation Report," *Verizon*, 2014–2021, May 19, 2021
3. "Cyentia Institute Publishes Groundbreaking Research on the Frequency and Cost of Breaches," *Cyentia Institute*, March 18, 2020.
4. "Cyentia Institute Publishes Groundbreaking Research," *Cyentia Institute*.
5. "Internet Crime Report 2020," *Internet Crime Complaint Center (IC3)*, March 17, 2021.
6. "Internet Crime Report 2021," *Internet Crime Complaint Center (IC3)* March 22, 2022.
7. "Internet Crime Report 2022," I*nternet Crime Complaint Center (IC3)*, March 7, 2023.
8. Petrosyan, Ani, "Cybercrime: Monetary Damage United States 2022," *Statista*.
9. "Annual Reports," *Internet Crime Complaint Center (IC3)*, 2013–2023.
10. Paganini, Pierluigi, "SolarWinds Hack: the Mystery of One of the Biggest Cyberattacks Ever," *Cybernews*, September 28, 2021.
11. Paul, Kari, "What You Need to Know About the Biggest Hack of the US Government in Years," *The Guardian*, December 1, 2020.
12. Gallagher, Ryan, "SolarWinds Adviser Warned of Lax Security Years Before Hack," *Bloomberg*, December 21, 2020.
13. Paganini, "SolarWinds Hack: The Mystery," *Cybernews*.
14. Kovacs, Eduard, "Class Action Lawsuit Filed Against SolarWinds Over Hack," *SecurityWeek*, January 6, 2021.
15. Whittaker, Zack. "SolarWinds Says it's Facing SEC 'Enforcement Action' Over 2020 Hack," *TechCrunch*, November 7, 2022.
16. "SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," *SEC.gov*, July 26, 2023.
17. Patterson, Lucas Austin, "This Company Was Hit with a Devastating Ransomware Attack—But Instead of Giving In, It Rebuilt Everything," *Time*, July 14, 2021.
18. "Ransomware: What it Is & What to Do About it," *IC3.gov*.
19. Patterson, "This Company Was Hit," *Time*.
20. Briggs, Bill. "Hackers Hit Norsk Hydro with Ransomware. The Company Responded with Transparency," *Microsoft News*, December 16, 2019.
21. StatusCake Team, "The Most Expensive Website Downtime Periods in History," *StatusCake*, July 28, 2020.
22. Vavra, Shannon, "Amazon Outage Cost S&P 500 Companies $150M," *Axios*, March 2, 2017.
23 Kollewe, Julia and Gwyn Topham, "British Airways Owner Loses £170m in Value After IT Meltdown," *The Guardian*, May 30, 2017.
24. Greenberg, Andy, "Hackers Remotely Kill a Jeep on the Highway—With Me in It," *WIRED*, July 21, 2015.
25. National Highway Traffic Safety Administration (NHTSA), Department of Transportation (DOT), "Cybersecurity Best Practices for the Safety of Modern Vehicles." *Federal Register 86 FR 2481*. January 12, 2021. 2481–2486.
26. National Highway Traffic Safety Administration (NHTSA), Department of Transportation (DOT), "Cybersecurity Best Practices for the Safety of Modern Vehicles Draft 2020 Update," *NHTSA*. March 15, 2021.
27. National Highway Traffic Safety Administration (NHTSA), Department of Transportation (DOT), "Cybersecurity Best Practices for the Safety of Modern Vehicles Draft 2022 Update," *NHTSA*, September 9, 2022.
28. Venter, Razvan, "UNECE Cybersecurity Regulation (R155): State of the Art and Relation with ISO 21434 and TISAX Standards," *Secura*, March 2022.
29. "UN Regulations on Cybersecurity and Software Updates to Pave the Way for Mass Roll Out of Connected Vehicles," *UNECE*, June 24, 2020.
30. "UN Regulations on Cybersecurity" *UNECE*, June 24, 2020.
31. Taub, Eric A., "Carmakers Strive to Stay Ahead of Hackers," *New York Times*, March 18, 2021.