

THE CYBER BATTLEFIELD

What to expect on the front line between cyberattackers and cyber defenders

Cyberattackers are increasingly dominating the cyber battlefield against cyber defenders. Novel multi-extortion techniques, ransomware as a service (RaaS), and unprecedented supply chain attacks have almost erased barriers to entry for hackers and expanded the cyber spoils "pie." Cyber defenders struggle to keep up with their opponents' advances. Cybersecurity is on board agendas but is often seen as a "hygiene" measure that is part of the IT budget. Much like challenges to global physical defense capabilities, cyber defenders must take significant steps to establish sustainable and agile fit-for-purpose cybersecurity capabilities to defeat their cyber opponents.

AUTHORS

Maximilian Scherr
Vincenzo Basile
Matteo Sironi
Tom Teixeira
Philipp Mudersbach
Dmytro Zaika

ON THE FRONT LINE: CYBERATTACKERS ARE GAINING GROUND

Cybercrime and ransom attacks have been on the rise and seem to be unstoppable. The increase in cyberattacks within the last 16 years is overwhelming. According to the Center for Strategic and International Studies (CSIS), the number of incidents with more than US \$1 million in losses jumped within the past 15 years from just 13 incidents in 2007 to a staggering 140 incidents in 2022. Meanwhile, Statista estimated the global annual cost of cybercrime in 2022 to be \$8.4 trillion, with ransomware attacks becoming increasingly popular among cybercriminals. And according to various reports, an average of 71% of businesses worldwide have been victimized by ransomware, and the average cost of such an attack was \$4.5 million in 2022, which does not include payments (see Figure 1).

Looking solely at the year-on-year change from 2020 to 2021, a report by Palo Alto Networks found the average ransom demand increased by 144% to \$2.2 million, with the average ransom paid by cyberattack victims up 78% to \$541,000. That report highlighted an 85% increase in victims during the same period, with 2,566 victims publicly posted on leak sites. This number is assumed to be even higher as victims are only posted on leak sites if they did not pay the ransom demanded by threat actors. That same report says the most targeted regions in 2021, based on absolute numbers, were the Americas (60%); followed by Europe, the Middle East, and Africa (31%); and Asia Pacific (9%).

The industries of manufacturing, financial services, professional/business services, education, healthcare, and governments are listed among the most heavily targeted industries by cyberattacks in 2021 and 2022 as reported by cybersecurity companies. The manufacturing industry in particular is undergoing a rapid Internet of Things (IoT) adoption due to increased digitization, offering a larger attack surface to threat actors. On top of that, costs of business disruption in manufacturing companies are elevated because their business has a low tolerance for downtime and continuity is highly dependent on IT and operational technology (OT) systems. According to an IBM Security report, this makes such sectors highly attractive to ransomware actors as they expect less resistance and faster ransom payments from the attacked companies. However, even leading tech companies, which could be expected to have extremely advanced cybersecurity measures in place, are not exempt from cyberattacks, as demonstrated by the attacks on Nvidia and Twitter in 2022.

Generally, the unprecedented increase in cyberattack incidents can be attributed to three key developments, as outlined below.

1. Technology expansion

As the world continues to become more connected, companies have seen an inherent increase in attack surface. The expansion of technology, driven mainly by Industry 4.0, IoT, digital transformation, smart manufacturing, and industrial automation, has led to the integration and deepening of connections between systems. Even though such connectivity delivers better use of data, efficiency savings, and productivity gains, it also offers favorable opportunities for threat actors to attack companies' systems due to the novel access points it creates.

Figure 1. Key cybersecurity figures, 2022



Source: Arthur D. Little, Statista, IBM

To illustrate in numbers: RiskIQ estimates that, every minute, 117,298 hosts (devices, such as computers or mobile phones, that link to other devices on a network) and 613 domains (unique website addresses) are being created and added to the global attack surface. During 2023, Cisco predicts the number of devices connected to IP networks will be more than three times the global population, increasing from 2.4 networked devices per capita in 2018 to an estimated 3.6 networked devices per capita. Similarly, Cisco estimates machine-to-machine (M2M) connections to comprise half the global connected devices and connections in this period, jumping from 33% in 2018 to 50% in 2023 (see Figure 2).

2. Sophisticated technology providers with integrated back doors

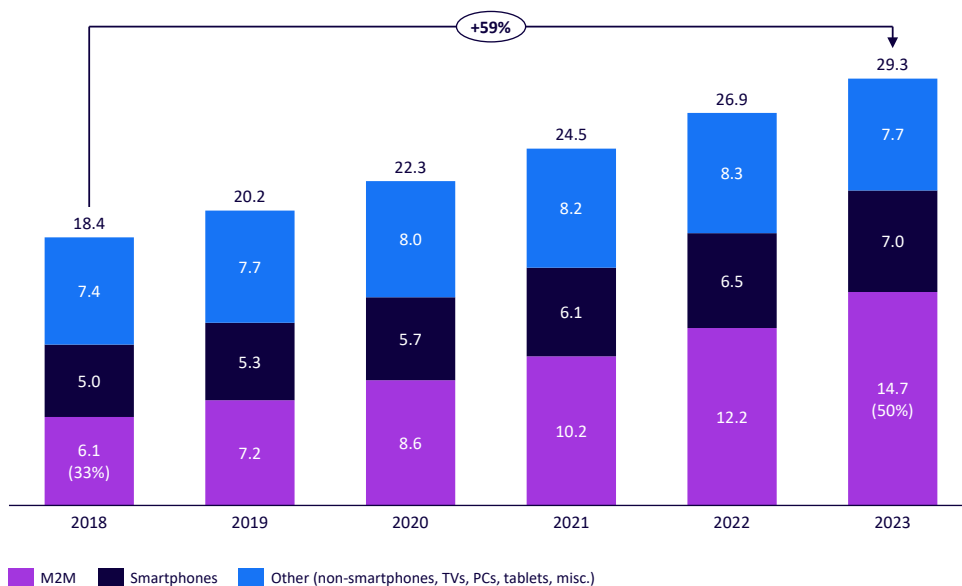
The 2020 SolarWinds attack, where a foundational IT infrastructure performance-monitoring system implemented by ~30,000 public and private organizations — including the US Treasury, US Homeland Security, and possibly NATO, among others — showed that supply chain monitoring, even with trusted suppliers, is required to ensure a comprehensive cyber risk picture. Incidents such as this one demonstrate that companies can also now be hacked indirectly through an open network when working with IT outsourcing providers.

3. Emergence of hybrid work

The COVID-19 pandemic and consequent global shift to working from home (WFH) further drove a rise in cyberattacks. Employees moved outside their organizations’ secure on-premise networks to their own home or, worst case, public networks and consequently increased the level of data and critical transactions flowing outside protected company local area networks. Furthermore, attacks have increased on remote services such as remote desktop protocols and virtual private networks (VPNs), as well as commercial and enterprise remote-meeting services due to inherent security flaws that have emerged based on organizations’ needs to adjust to WFH. A similar picture exists for cloud-based services, which indeed provide more flexibility and performance than traditional VPN connections but often offer increased attack surface due to poor and hasty security implementations. These developments have put increased responsibility on cyber defenders to ramp up their companies’ cyber defenses.

Analyzing the motives, tools, and trends of cyberattackers and cyber defenders provides a better understanding of the battlefield.

Figure 2. Number of connected devices globally, 2018–2023



THE REALM OF CYBERATTACKERS

While there are new cybercrime groups emerging every year, the biggest share of cyberattacks are both known and reemerged actors. Within the realm of ransomware attacks that took place in 2021/2022, the most prominent groups are Conti, REvil/Sodinokibi (which successfully reemerged in December 2022 after many members were arrested a few months earlier in May), Black Basta (consisting of former members of Conti and REvil), ALPHV/BlackCat, Hive, and LockBit (also a reemerged group). A big share of these organizations regularly make it into the headlines of mainstream media as they are often responsible for some of the most destructive attacks.

According to a 2022 report by Palo Alto Networks, many of these threat actors started with comparatively low ransom demands, mostly below \$1 million, and quickly ramped up to more than \$5 million. As stated earlier, the average ransom demand grew by 144%, and the average payment increased by 78% from 2020 to 2021. However, victims paid only an average of 43% of the initial ransom amount, and there were incidents in which the amount paid was more than 70% lower than the ransom demanded.

Ransomware groups are getting increasingly professional and commercial through RaaS and hacking as a service, forming organizational structures with sophisticated affiliate systems. Threat actors also are getting more ruthless, utilizing double- and multi-extortion techniques (see “Trend 1 – Double & multi-extortion” below).

Even though such threat actors are criminals, there has always been a certain “code of honor,” such as not targeting hospitals, emergency services, or law enforcement. However, a growing number of groups have been disregarding this code. A prime example is Conti, which has targeted hospitals and emergency services. Additionally, they ignored their promises and published sensitive data when victims had paid them not to. Problems have been exacerbated by the recent increase in geopolitical risks.

Ransomware activities: Increasingly sophisticated & commercial

Trend 1 – Double & multi-extortion

Not only has the number of incidents risen starkly over the past year, attacks have also become more multilayered. Historically, ransom attacks were seen just as an availability problem; attackers only encrypted and locked victims out of their data. Cyberattacks have advanced, however, and are now frequently a confidentiality problem as well. In addition to encrypting the victim's data, since 2020, threat actors have increasingly added double- and multi-extortion techniques to their repertoire (see Figure 3). Adversaries are now actively exfiltrating their victims' data, threatening to publicly name and shame them, and posting their data on so-called leak sites should victims not agree to pay the ransom. They even threaten their victims with additional follow-on attacks, such as distributed denial-of-service (DDoS) attacks, and so on, resulting in multi-extortion attacks.

To address this trend, every company must force itself into thinking differently about cybersecurity, assuming it has already been hacked and now needs to respond to advanced persistent threats placed on its systems and that only wait to be activated at the best moment as the basis for multi-extortion attacks.

Figure 3. Double- & multi-extortion techniques



Source: Arthur D. Little

Trend 2 — Commercial RaaS

The increase in attacks has also been driven by the development of commercial RaaS offerings (see Figure 4). Threat actors have been building ransom software that can be bought by aspiring attackers who might not have the knowledge to build their own tools. This market development has made ransomware much more accessible to cybercriminals who want to get a piece of the growing pie. RaaS is often exchanged based on monthly fees, just like the usual Spotify or Netflix subscriptions, or by a percentage of the ransom victims pay.

Considering the low barriers to entry, attacks might increase in number but not necessarily in sophistication. Basic hygiene through cybersecurity-awareness training, regular updates of security policies, threat protection on emailing infrastructure, and rigorous vulnerability management will help effectively address these threats.

Trend 3 — Software supply chain attacks

Recent developments have shown how important it is to take a closer look at a company’s own software supply chain (see Figure 5). Software supply chain attacks have risen significantly — almost tripling from 2020 to 2021, according to Aqua Security. Recent major attacks include SolarWinds and Kaseya. The primary foci of such attacks are open source vulnerabilities and poisoning, code-integrity issues, and the exploitation of software supply

chain processes and supplier trust. Cyberattackers are especially targeting managed service providers, as such types of technology management solutions can have high concentrations of risk due to their large collection of enterprise accounts with elevated privileges, unrestricted firewall rules needed for them to operate, and a cultural trust that the traffic to and from them is legitimate and should be allowed.

Releasing supply chain security policies, ensuring approvals through a cybersecurity department prior to giving access to a new supplier, and regularly monitoring supply chain through cybersecurity-rating platforms such as BitSight, SecurityScorecard, or others are essential tools for preventing cyber risks up or down the supply chain.

THE REALM OF CYBER DEFENDERS

There is a strong asymmetry in the cyber war. Adversaries are adapting and developing faster than cyber defenders. Defenders are facing three central challenges (see the Arthur D. Little [ADL] Viewpoint, “[Being Concerned Is Not Enough](#)”):

1. **Visibility and understanding at board level.** There is an inherent complexity within cybersecurity that is hard to translate into understandable, action-oriented recommendations for top management. To address the issue, companies turn to commonly applied standards within IT and OT cybersecurity, such as ISO 27001 and IEC 62443, to benchmark cybersecurity best practices. However, the key challenge is to strike a balance between maintaining the required technical level of details while achieving general comprehensiveness, especially for top-level decision makers and budget holders.
2. **Resource allocation/funding.** There has been an apparent mismatch between the economic damage of cyberattacks and their cybersecurity investments. In 2021, the global cost of cybercrime-to-global-cybersecurity-investments ratio amounted to just 10:1.

Figure 4. Ransomware as a service



Source: Arthur D. Little

Figure 5. Software supply chain attacks



Source: Arthur D. Little

That means, for example, that for every \$1 spent on addressing a breach of a company's network, only \$0.10 is invested to prevent potential future compromise. Our view is that going forward this ratio has to be inverted: spending on prevention and remediation of advanced persistent threats will need to be significantly increased, posing additional challenges for sufficient funding within organizations.

- 3. Measurement.** Calculations of ROI indicators of a cybersecurity program are especially complex, as returns can only be reflected as the opportunity cost of damages from a cyberattack or an estimated value of cyber risk documented by corporate risk and compliance.

These three root problems have given rise to significant technical challenges. Cyber defenders struggle to detect and disrupt threat actors' activities and climb to the top of cybersecurity expert David Bianco's "Pyramid of Pain" due to the ever-evolving skill sets of attackers (see Figure 6). Not all indicators of harmful activities are equal and some are more valuable than others because they cause more "pain" to threat actors when they are denied to them by cyber defenders. Indicators at the bottom of the pyramid are easy to detect and get hold of, such as hash values, IP addresses, and domain names. Denying a threat actor a certain IP address will not be much of an obstacle, as they can easily create and use a

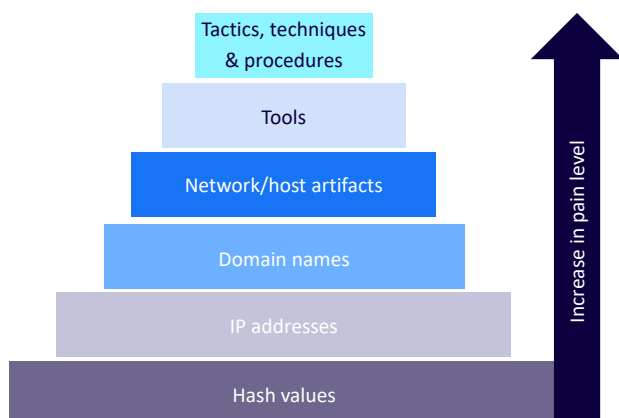
different address. However, as cyber defenders move up the pyramid, they create more obstacles for cyberattackers. These indicators are harder to detect and block. Denying the attacker the use of tools and even TTPs (tactics, techniques, and procedures) will force them either to give up or invest significant time into finding or developing a new tool to penetrate the victim's system — meaning more time for cyber defenders to stop the cyberattack on their systems. At the same time, cyber defenders and their companies face increased responsibility from a variety of angles to prepare against cyberattacks.

Accountability rising from EU regulations

The EU has increasingly put measures in place to weather cyberattacks. With the EU Cybersecurity Act, the EU has strengthened its Agency for Cybersecurity (ENISA) and established a cybersecurity framework for products and services. The act introduced an EU-wide framework for information and communication technology (ICT) offerings that enables businesses to certify their ICT products, processes, and services only once and see their certificates recognized across the entire EU.

Furthermore, the European Commission has presented a proposal for the Cyber Resilience Act, which introduces mandatory cybersecurity requirements for hardware and software products throughout their whole lifecycle and results in tougher rules for makers of products with digital elements. Companies will have to ensure that their products have fewer vulnerabilities and will remain responsible for cybersecurity throughout a product's lifecycle. The act also improves transparency on security of hardware and software, as cybersecurity risks must be documented and actively exploited vulnerabilities and incidents reported. Ultimately, business users and consumers will benefit from better protection. According to the *Financial Times*, failing to comply with the act is expected to result in a fine of up to €15 million (~\$16 million) or 2.5% of the previous year's global turnover, whichever is higher. The act is expected to become law by 2024.

Figure 6. Pyramid of Pain



Source: Arthur D. Little, David Bianco

Increased efforts & prerequisites to access cyber insurance

The increase in attacks and their consequent damages have prompted a turn toward cyber insurance even though general cyber insurance does not cover ransom payments, only damages. However, insurers face major challenges in how best to deal with the most extreme forms of risks, such as major state-backed attacks or attacks across a large number of clients and with cyber-physical events that begin in the digital space but have major impacts on society. In recent years, insurers have been unwilling to pay claims for major cyberattacks, such as NotPetya, as they argue that state-backed attacks are acts of war and as such are excluded from their cybersecurity coverage. This means that companies seeking cybersecurity coverage will need to understand what is and is not covered by insurance and consequently how to adequately ensure and manage protection of areas not covered by insurers. Furthermore, companies are facing increasingly strong prerequisites from insurers to gain access to favorable cyber policies.

Cybersecurity awareness & training

Cybersecurity awareness and training become increasingly relevant, and we expect that cybersecurity-awareness trainings will become a legal requirement in the majority of the developed world in the very near future. Nevertheless, the sooner such trainings are implemented across companies, the less cyber risk will be observed.

A more dynamic, agile approach to cyber defense









Trend 1 – Shifting to indicators of behavior

Cyber defenders have been shifting toward ex ante behavioral telemetry and indicators of behavior (IoBs) instead of often ex post indicators of compromise (IoCs), as there are substantial problems connected to IoCs, including (as defined by Cyberreason CSO Sam Curry):

1. Attackers are more advanced and are likely to not reuse codes they had successfully used before. Therefore, keeping old indicators and looking for them in company systems will no longer help protect against new cyberattacks.
2. Attackers sometimes intentionally inject noise into the IoC system by sending masses of false artifacts to IoC databases, making it difficult for defenders to find the signal in their own cyber backyards. As an example, attackers will drop files into the IoC ecosystem with no purpose other than to drive up the noise-to-signal ratio and give them an opportunity to trigger false positives in new sites.
3. Attackers do not only use their own external code as means of attack anymore. Instead they use benign software and exploit security issues within these trusted applications to breach and gain access to their victims' systems.

Although IoCs have a low false-positive rate, they are static and backward-looking, as they are point-in-time references (e.g., IP addresses, file names, or hashes — see Figure 7) to isolated hostile actions that are constantly changing, resulting in low efficacy against new and evolved cyberattacks.¹ Behavioral telemetry and IoBs, however, can identify such new attacks, as they monitor and analyze current behaviors and user patterns happening in real time in the system to flag potential security threats and system breaches. More specifically, IoBs focus on the approach of an attack. They are chains of behavior or processes that behave differently and stand out from other behaviors in an organization or are statistically rare (e.g., unusual updates in

Figure 7. Examples of indicators of compromise vs. indicators of behavior

COMPROMISE EXAMPLES	BEHAVIOR EXAMPLES
 IP addresses/file names/ hashes ...	 Unusual updates in software
 Large numbers of requests for same file	 Modification of scheduled or standardized tasks
 Uncommon outbound network traffic	 Large download of data to a removable storage device
 Data bundles in unusual places	 Uncommon access of stored information

Source: Arthur D. Little

¹ Hedrick, Shaun. "IOCs vs. IOAs: How to Effectively Leverage Indicators." Security Intelligence, 16 March 2022.

software or the modification of scheduled tasks — see Figure 7).² Compared to retrospective IoCs, IoBs can thus detect intrusion patterns that are less obvious and identify adverse activity prior to a successfully completed attack.³ However, they show a high false-positive rate due to their inherent characteristics of being more proactive and dynamic than IoCs. The next level in cybersecurity will build on a combination and correlation of IoCs and IoBs, to yield new, dynamic, and situational alarms with low false-positive rates.

Investing in the latest cybersecurity tools, such as best-in-class security operation center (SOC) services, extended detection and response capabilities (XDR), and zero trust with secure access service edge (SASE) will help to proactively track and respond to threats before any system has been compromised.

Trend 2 — Cyberattacks have evolved into chains of behaviors

Rather than thinking about cyberattacks as one particular moment, there has been a shift to see attacks as chains of behavior that usually look benign but can turn malign. Furthermore, attackers are becoming increasingly persistent in their attacks, resulting in a growing number of attacks as well as longer attack chains.

As shown in Figure 8, which depicts an extension of the so-called MITRE ATT&CK Matrix describing a structured list of known attacker behaviors, cyberattacks are now seen as chains comprised of many different parts and steps, such as reconnaissance, resource development, initial access, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, command & control, impact, exfiltration, and cleanup.

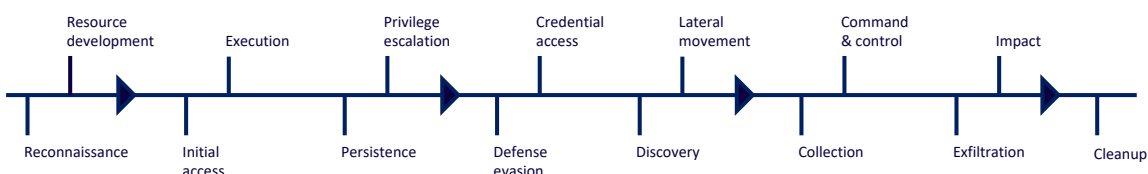
escalation, defense evasion, credential access, discovery, lateral movement, collection, command and control, exfiltration, impact, and cleanup. Although cyberattack chains are not the only way to understand attack points and security risks, they allow cyber defenders to get better at preventing and disturbing attacks as well as minimizing the impact of such breaches due to the more granular approach taken.

“Know thyself, know your enemy”: a comprehensive view on likely enemies’ behavior and understanding whether there are enough implemented cybersecurity controls to address each potential escalation action will help a company take the next step in its cybersecurity stance and identify hacks-in-progress along the cyberattack chain. One of the best tools to enable a comprehensive high-level view on cybersecurity is total cost of cybersecurity risk, which enables senior management to make decisions based on the overall financial exposure. ADL sees three key elements within cyber risk exposure:

1. **Data breach costs** — for example, fines and costs of notifications resulting from personally identifiable information (PII) being leaked.
2. **Ransom versus recovery costs** — do you pay ransom, trusting the hacker, to quickly restore operations, which might be legally problematic in some jurisdictions, or do you develop a resilient recovery/restore procedure guaranteeing certain recovery time and recovery point objectives to business?
3. **Business disruption costs** — for example, a “price tag” for each hour critical systems are down.

² Curry, Sam. “SolarWinds Attacks Highlight Advantage of Indicators of Behavior for Early Detection.” Cyberreason, 27 January 2021.
³ Hedrick, Shaun. “IOCs vs. IOAs: How to Effectively Leverage Indicators.” Security Intelligence, 16 March 2022.

Figure 8. Extension of the MITRE ATT&CK Matrix — Cyberattacks as chains of behaviors



Source: Arthur D. Little, MITRE ATT&CK

These factors can be multiplied by the probability of being hacked, which is, in part, a subjective assessment based on maturity of the cybersecurity domains; key cybersecurity KPIs like vulnerability count on IT infrastructure; and the overall threat landscape, which varies depending on industry and geography.

Trend 3 — OT cybersecurity as a new focus

Cyberattacks on OT have been increasing over the last years, with prominent attacks such as Colonial Pipeline and SolarWinds resulting in significant physical impact on companies and society. OT systems are highly complex and their segregated technology, machinery, and equipment are sensitive to external devices. On top of that, many systems are 30–40 years old and not designed to connect to wide area networks.

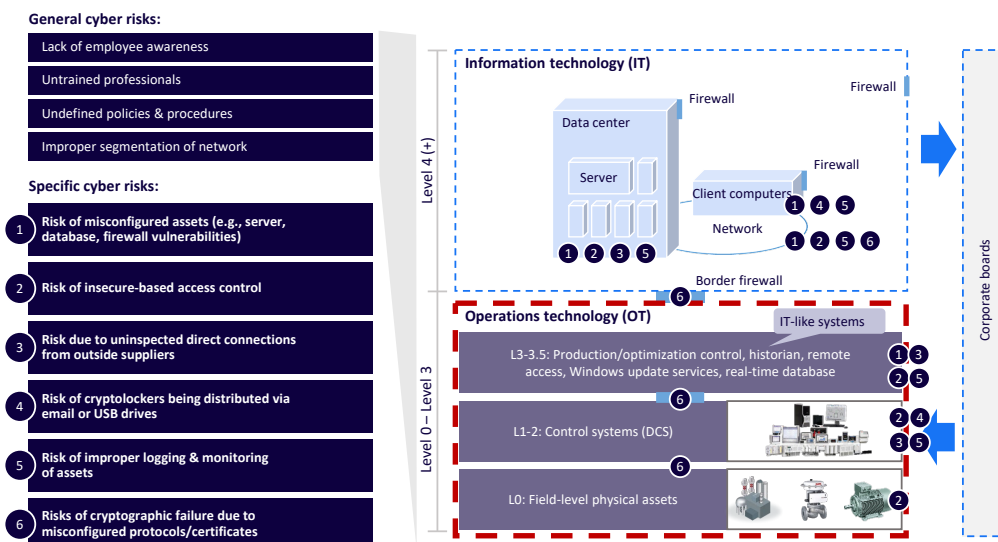
Since the most recent attacks were executed via breaching software supply chains, cyber defenders are now focusing increasingly on supplier assurance due to the current inability to ascertain security practices of third parties. Furthermore, demand for software bills of materials and implementation of cybersecurity requirements in software supplier contracts have risen. Despite the availability of enabling technologies such as automation, machine learning, orchestration, and artificial intelligence, there has been a slow adoption rate for these advances, as companies believe that such

technologies are not yet mature enough to produce the impact required. Instead, companies are still focusing on and improving known technologies, such as OT patch management, secure remote access, industrial firewall, and OT inventory and asset management systems.

A report by Applied Risk estimates that OT security development over the next two to four years will be driven by expansions of general workforce skill pools and OT security headcount, IT/OT convergence, as well as by SOCs, which are centralized functions or teams that monitor an organization’s entire IT infrastructure 24/7 and are usually responsible for preventing, detecting, and responding to cyberattacks. Indeed, OT will see a stronger IT/OT convergence driven by, for example, industrial IoT, which is expected to be an accelerator for creating cross-functional IT and OT security teams achieving cybersecurity convergence and more efficient mitigation of cybersecurity risks, especially since both IT and OT incur often similar cyber risks at different architecture levels, as illustrated in Figure 9.

Akin to IT security, a comprehensive up-to-date view on the OT asset database — with a focus on connected assets, especially IoT devices — is required as the foundation to act in the OT area. A number of OT-focused cybersecurity suppliers are emerging (e.g., Otorio) that will help document and monitor the OT assets and also actively manage risk and respond to potential threats.

Figure 9. Enterprise IT & OT architecture levels and their related cyber risks



Source: Arthur D. Little, Purdue Enterprise Reference Architecture

CONCLUSION

TAKING ON THE THREAT

MODERN CYBERSECURITY REQUIRES DEVELOPMENT AND OPERATIONS TO GO HAND IN HAND

It is time for cyber defenders to start winning on the battlefield. First and foremost, understanding the cybersecurity risk exposure is key to enable a comprehensive battlefield view. Second, agility in both strategic and tactical cybersecurity measures is indispensable to address ever-evolving threats from cyberattackers. It is not enough to “close the gap” in cybersecurity capabilities once; much like in software development, modern cybersecurity requires development and operations to go hand in hand, ever updating both cybersecurity strategy and the toolset to respond to current challenges while ensuring excellence in day-to-day operations. We recommend that companies take five steps to establish sustainable, agile, fit-for-purpose cybersecurity capabilities:

- 1 Engage an objective expert view on the status quo of the organization’s total cost of cybersecurity risk.** We advise working closely with risk management to understand cost of business disruption due to IT or OT systems being compromised as well as costs of a potential PII data breach. Additionally, a comprehensive

cybersecurity maturity assessment should ensure the understanding of the probability of a breach and allow the necessary level of granularity while still providing readily understandable insights and priorities for the C-level audience.

- 2 Ensure definition and oversight of the organization's key indicators for cybersecurity performance.** Both leading and lagging, providing assurance that the controls in place are offering the right level of protection.
- 3 Review fact-based and unvarnished updates.** Periodic review not only facilitates progress tracking but also ensures that resources are allocated in the most effective way for reaching the intended maturity level.
- 4 Provide cybersecurity-awareness training.** Regular company-wide training should include conventional presentations and booklets as well as fake internal phishing campaigns to monitor awareness indicators and take actions against continuous negligence.
- 5 Get more agile.** To weather the ever-evolving tools of cyberattackers, defenders will need to be more agile by switching from static and reactive measures to proactive and dynamic acts of cyber defense, enabling the rate of improvement and faster detection and threat combat.



Arthur D. Little has been at the forefront of innovation since 1886. We are an acknowledged thought leader in linking strategy, innovation and transformation in technology-intensive and converging industries. We navigate our clients through changing business ecosystems to uncover new growth opportunities. We enable our clients to build innovation capabilities and transform their organizations.

Our consultants have strong practical industry experience combined with excellent knowledge of key trends and dynamics. ADL is present in the most important business centers around the world. We are proud to serve most of the Fortune 1000 companies, in addition to other leading firms and public sector organizations.

For further information, please visit www.adlittle.com.