



DISCLOSURE IS NOT LIMITED

# Securing the modern pharmaceutical supply chain

**A guide for CISOs in an age of disruption**

November 2021

[kpmg.com](https://www.kpmg.com)

DISCLOSURE IS NOT LIMITED

To all contributors,

I would like to extend my deep appreciation for the incredible support provided to bring this paper to life. Despite busy schedules and myriad other commitments, you have provided your time, knowledge, and expertise to produce immense value for the H-ISAC community. Your commitment to advancing the security of the industry has helped to better shape the future of collaboration among existing and future members. For this I am truly grateful.

Serving at the helm of this group effort, from ideation back in June to delivery at the H-ISAC Fall Summit, has truly been a pleasure. The team naturally brought a wide diversity of backgrounds and opinions, which played a major role in delivering a valuable perspective. I hope that readers will take away insights they can use in their own environments to secure the supply chain and improve the ecosystem.

Thank you once again for all your contributions, and I look forward to working with you on future efforts.

Sincerely,

Mike Wagner



DISCLOSURE IS NOT LIMITED

# Contents

**Executive summary**

**2**

**Introduction**

**3**

**A unique role in the modern pharmaceutical organization**

**4**

**A different type of technology leader**

**6**

**Top six cybersecurity threats on pharma CISOs' minds**

**7**

**Key cybersecurity principles for countering the top six threats**

**12**

**Conclusion**

**16**

**Participating CISOs**

**17**

**Contributors**

**19**



DISCLOSURE IS NOT LIMITED

Securing the modern pharmaceutical supply chain



# Executive summary

**Members of the Health-ISAC community have produced a security framework for the pharmaceutical supply chain comprising this CISO guide, as well as a practitioners' guide presenting best practices, and recommended cybersecurity standards, across the key links in the pharmaceutical industry. Led by Johnson & Johnson and facilitated by KPMG, the cross-institutional team comprises CISOs and subject matter experts from J&J, Pfizer, Cardinal Health, McKesson, Abbott, and Eli Lilly and Company.**



**DISCLOSURE IS NOT LIMITED**



**DISCLOSURE IS NOT LIMITED**



DISCLOSURE IS NOT LIMITED



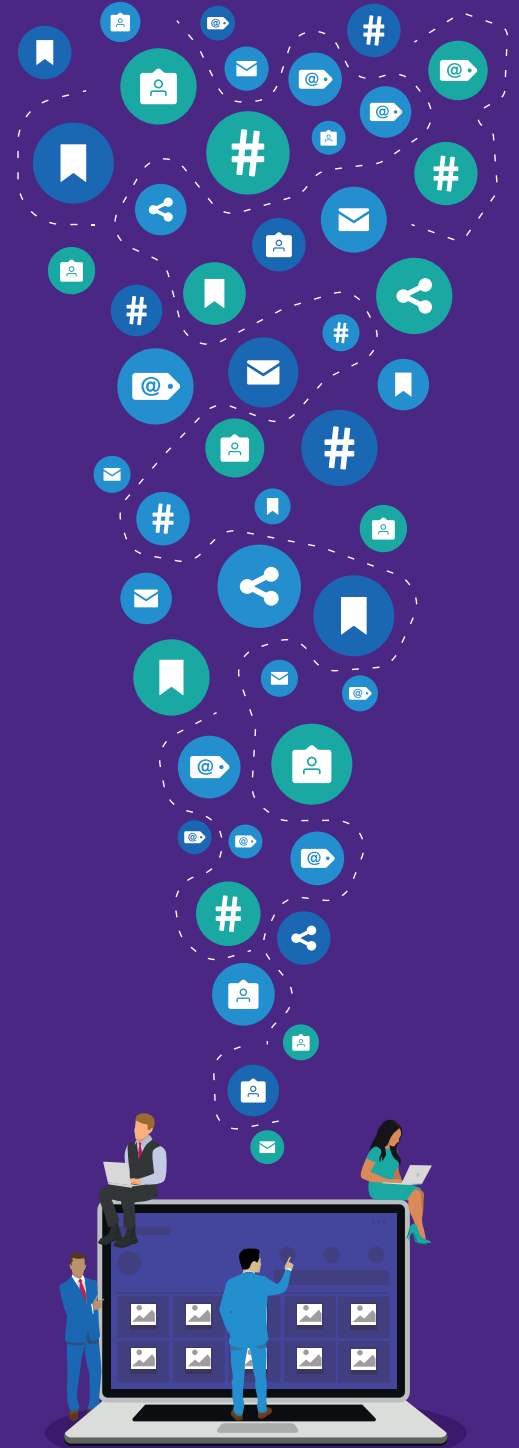
# Introduction

**Although the pharmaceutical industry was vulnerable to ransomware attacks and intellectual property (IP) theft before the pandemic, drug manufacturers have certainly moved higher on the list of potential targets of cyber-crime. Headline-grabbing COVID-19 vaccines and treatments, as well as lucrative biologics and perennial brand-name drugs, have called attention to pharma companies' financial reserves and valuable intellectual property.**

At the same time, the number of attack vectors has increased exponentially due to (1) the digitalization and increased complexity of the pharmaceutical supply chain and (2) industrywide dependence on a growing array of foreign and domestic third-party suppliers and partners with varying degrees of cyber maturity.

These factors and others explored in this paper have made securing the supply chain an organizational imperative. And chief information security officers (CISOs) are earning a much more strategic seat at the table: They are being asked to weigh in on how the business can pursue efficiency, productivity, and even growth initiatives without taking unnecessary reputational, financial, or regulatory risks.

In other words, CISOs and their teams have shifted from the sidelines to, if not center stage, at least a key part of the ensemble.



DISCLOSURE IS NOT LIMITED



DISCLOSURE IS NOT LIMITED



# A unique role in the modern pharmaceutical organization

**All CISOs interviewed for this paper stressed the importance of tying security and technology solutions to the economics of the business.**

Today's pharmaceutical CISO is in a unique position straddling technology and the business. On the one hand, CISOs need to maintain consistent cybersecurity standards and protocols across not only information technology (IT), but also operational technology (OT) and third parties. On the other hand, they need to speak the language of the business so they can present emerging risks in a context that will resonate and serve as a catalyst for support from the leadership team.

Both sides benefit if cybersecurity teams can understand business priorities and calibrate their cyber programs to align with the potential economic or reputational impact of a company breach. For example, preventing theft of intellectual property (IP) from an R&D lab may be a higher priority than averting a breach of a stand-alone technology stack.

While speaking the business's language is a path to more meaningful leadership, the need for effective communication cuts both ways, i.e., business leaders must be better versed in crisis and risk management as well. In an ideal world, for every question that cybersecurity had about strategic plans, senior executives would have just as many about how security concerns impact their decision-making.

Brian Cincera, senior vice president and CISO, Pfizer, corroborates this view: "Effective CISOs understand the full range of key business processes and can quickly evaluate existing and emerging risks to advise business leaders on directions to take. Cybersecurity has earned a seat at the table when organizations are planning and executing critical processes, including those related to the supply chain."



**I have been a CISO at J&J for nearly 11 years. For most of that time, I was beholden to a defense model, reacting to advanced persistent threat groups. The difference today is that, with digitalization, if cyber-attackers come in an organization's back door, they can get to almost everything. Therefore, it is critical that cybersecurity teams shift to a proactive approach that is closely tied to the business.**



**—Marene Allison**  
CISO, Johnson & Johnson



DISCLOSURE IS NOT LIMITED



DISCLOSURE IS NOT LIMITED



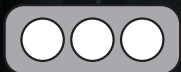
Developing COVID-19 therapies fast couldn't include cutting corners, including in managing cyber risks. Executives demanded both moving fast and assuring full control compliance. Expanding our view of risks to include the full supply chain helped us more quickly identify risks and knock down barriers to bringing therapies to patients.



— Brian Cincera  
Senior Vice President and  
CISO, Pfizer

The pandemic highlighted the wisdom of giving cybersecurity a seat at the table in relation to decisions surrounding mergers & acquisitions and partnerships. Leaving cybersecurity out of the due diligence process when pursuing acquisitions of small companies, especially when they are key suppliers/partners or sole sources, is like flying on a trapeze without a net. In fact, with any acquisition, if it is revealed post deal that a company's cybersecurity program doesn't pass muster, CISOs and their teams will likely need to perform extensive remediation and the company could face liability for damages if sensitive information is compromised.

It is equally important to have cybersecurity weigh in on potential partnerships and joint ventures, such as those that offer peripheral products and services to aid production and distribution. During the pandemic response, many companies eschewed some partnerships after CISOs and their teams uncovered cyber risks. Instead, they bought or built components of the supply chain, such as cold chain storage, themselves.



DISCLOSURE IS NOT LIMITED





DISCLOSURE IS NOT LIMITED



# A different type of technology leader

**The view of the CISOs interviewed for this paper is that their position has evolved from a supportive internal role to a highly visible role both internally and externally.**

At the same time as modern pharmaceutical CISOs interface regularly with the business, they are now engaging in a fair amount of external outreach as well. They must be tuned into not only what it takes for their organizations to run, but also what it takes for their industry to thrive. Many of the CISOs surveyed for this paper feel that evolving industry and societal dynamics are driving them to be more vocal, bold, and transparent than they were, perhaps, accustomed to. They are expected to offer a perspective on how to keep the supply chain and other operations running safely throughout the pandemic and to predict what the top security concerns will be after we emerge from this global health crisis.

Regarding whether there will be sufficient talent as cybersecurity needs continue to evolve, many CISOs view it as their responsibility to provide leadership when it comes to diversity and inclusion (D&I) and mentorship to help guide future cyber professionals.

Lori Havlovitz, CISO, Cardinal Health says her company sets a very high bar when it comes to the commitment to hiring and nurturing diverse teams: "We are committed to having a diversity of voices on our teams and offering opportunities for unconventional talent to enter the cybersecurity field. We truly believe that diversity of background goes hand in hand with diversity of thought."

CISOs understand that it is imperative to engage with students interested in STEM when they are kids and educate them on potential careers in the technology field.

By the time they get to college, it's too late. That is not to say that CISOs' leadership and guidance aren't needed at the university level. Many CISOs consult to college curriculum boards on the skills employers are seeking and stress the importance of incorporating active lab engagement along with theory.



**Demonstrating strong leadership as a CISO of course includes ensuring our cybersecurity protocols are as strong and comprehensive as they can be. But I believe we can have an external impact as well. Particularly when it comes to educating and inspiring employees and peers on issues related to diversity and inclusion and having transparent discussions on injustice in corporate America.**



**—Meredith Harper**  
Vice President and CISO,  
Eli Lilly and Company



DISCLOSURE IS NOT LIMITED

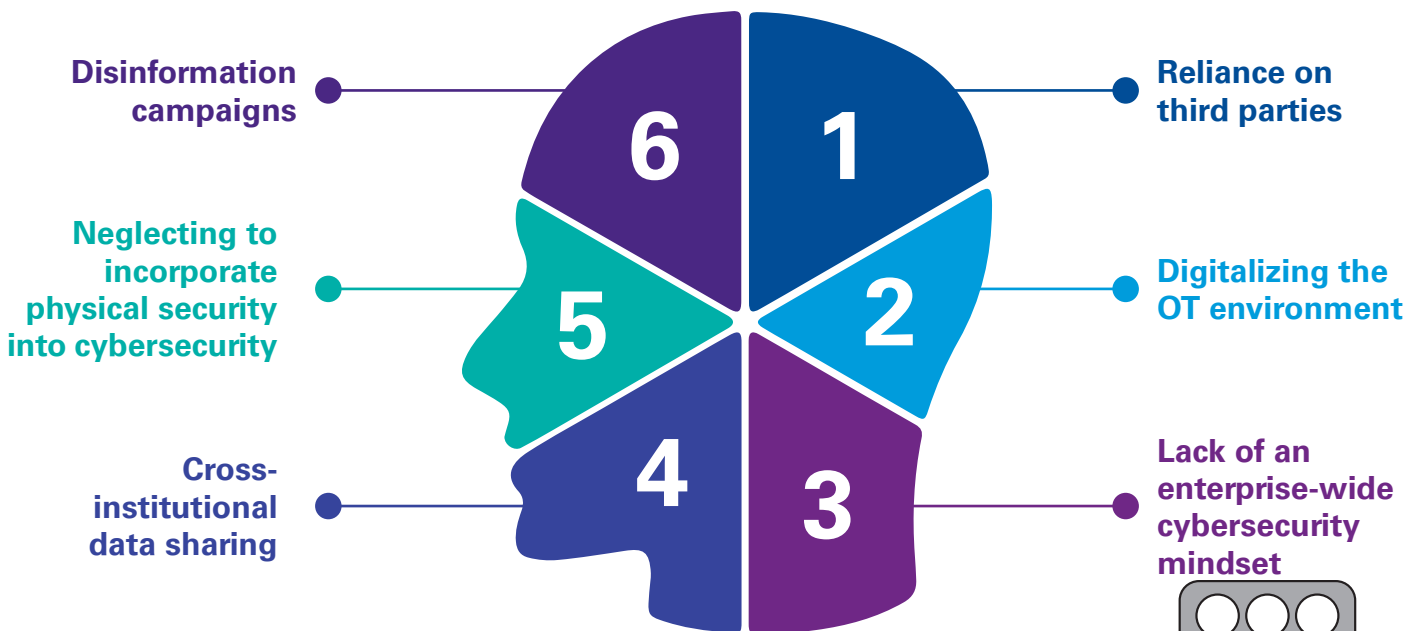




# Top six cybersecurity threats on pharma CISOs' minds

CISOs and their teams have a macro view of the most significant threats to the pharmaceutical supply chain. From the infusion of digital into processes and applications, to threats that arise around the connection between IT and OT, to aging legacy systems, the attack surface that can be exploited by threat actors is larger than ever. And the potential consequences of a breach have taken on increased weight in a time when disruption to the supply chain could delay delivery of lifesaving therapies, vaccines, and treatments.

Following is an overview of the top six cyber threats identified by CISOs interviewed for this paper, as well as some tips on contextualizing these risks for business leaders:





1

### Reliance on third parties

One of the biggest threats on CISOs' minds stems from their organizations' necessary dependency on third-party suppliers coupled with insufficient transparency into suppliers' cybersecurity protocols.

If a third party is breached, there could be a multitude of sub-optimal outcomes for pharmaceutical firms. For example: (1) A cyber-attacker could use a third party's software running on the organization's systems to introduce a virus or gain access to IP or patient data. (2) If a third party is out of commission, pharma companies would likely divert their business to alternate suppliers. However, if multiple pharmaceutical firms use the same suppliers, there could be significant supply and demand issues, including rationing of drug components. (3) And, in the case of sole suppliers, a breach could mean long-term shortages of lifesaving drugs.



**Key message for the business:** Aside from large distribution companies with high cyber resilience, most third-party suppliers are small businesses with a limited ability to invest in robust cybersecurity programs. Therefore, it is critical to conduct a thorough due diligence process before partnering with or acquiring a supplier.

*[For more, see "Hold third parties to a higher standard," page 13.]*






2

**Digitalizing the OT environment**

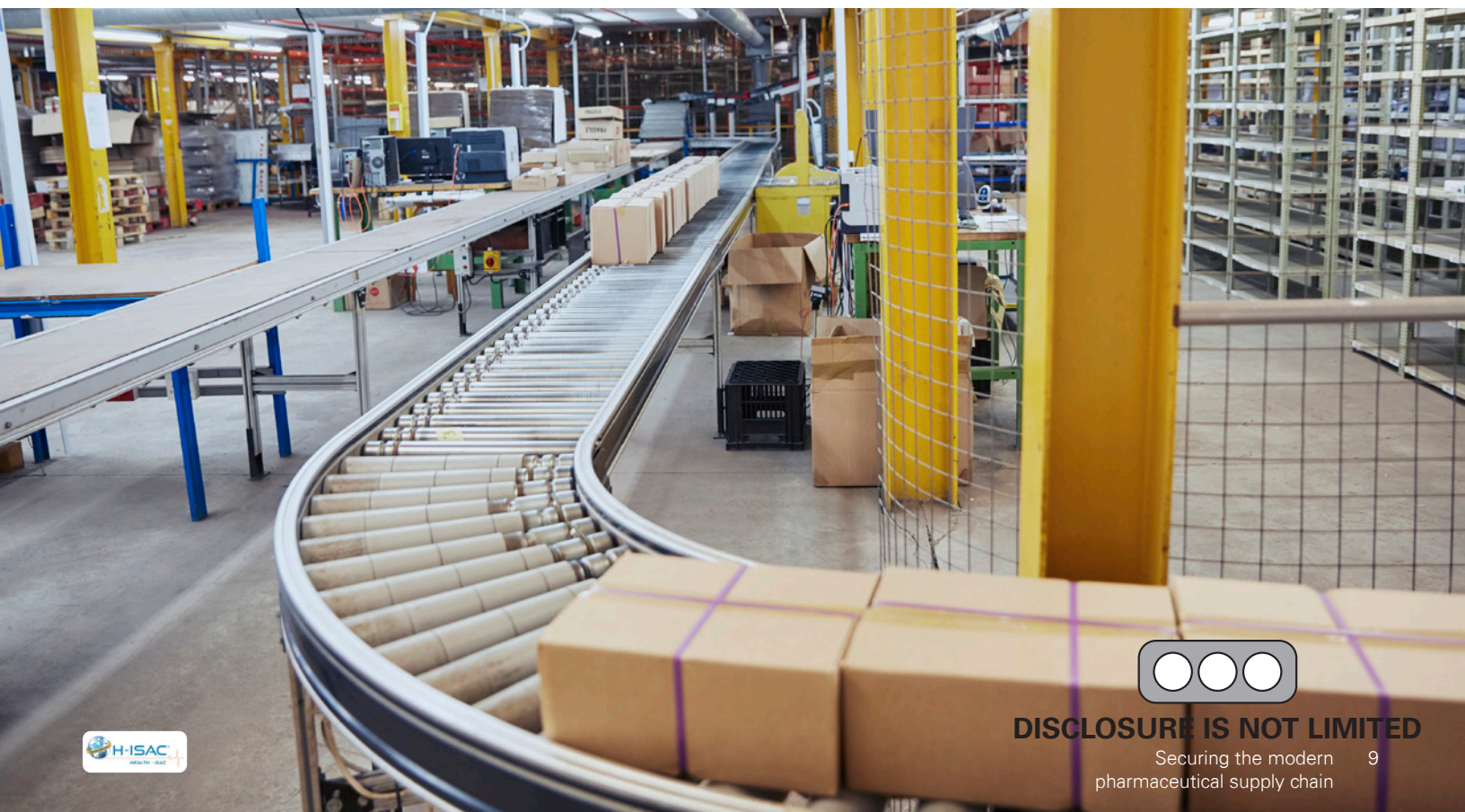
Since the traditional focus of pharmaceutical cybersecurity has been on protecting IT systems where patient data and IP are held, many pharmaceutical organizations lack well-developed OT cybersecurity measures. Industrial control systems (ICS)—running the manufacturing floor, distribution centers, R&D facilities, and labs—are no longer siloed from corporate networks. Patient data and drug formulas used in the manufacturing environment now run the risk of being part of the attack surface. OT environments where biologic drugs are manufactured are attractive targets for state-sponsored threat actors, who are very interested in IP and trade secrets related to these drugs.

Digitalizing the OT environment – while extremely valuable in terms of increased productivity, fewer production errors, and insights from operational analytics – could also make the organization more vulnerable to a cyberattack. The cloud, 5G technologies, blockchain, artificial intelligence, and the Industrial Internet of Things (IIoT) could inadvertently open new attack vectors for cyber criminals. IIoT, for example, poses an emerging threat as it is “always on” and could provide a bridge between OT assets and corporate networks.

When disruption occurs, it is difficult and time-consuming to bring OT/ICS systems back online and costly to replace or rebuild them. And companies are often slow to launch their response and recovery efforts after an OT attack as most don’t have a formalized cybersecurity infrastructure for their industrial environments or sufficient transparency into impacted assets.

 **Key message for the business:** Since OT systems have a higher dependency on reliability and availability than IT, an attack on the OT environment could prevent drugs from getting into the hands of customers including pharmacies, hospitals, and, of course, the patients who need them. It is, therefore, critical to prioritize the systems that hold the most sensitive and valuable data, as well as those where a breach could significantly disrupt drug manufacturing, i.e., the “crown jewels.”

*[For more, see “Focus on protecting the ‘crown jewels,’” page 13.]*





3

**Lack of an enterprise-wide cybersecurity mindset**

Many cyberattacks stem from human error, susceptibility to social engineering ploys, and insufficient identity access management controls. And yet, employees don't fully understand their own roles in protecting their organizations.

In fact, if organizations only provide periodic cybersecurity training, employees are left with only a rudimentary idea of how to be vigilant for potentially suspicious activity. And for the wide variety of organizational roles that now include cybersecurity hygiene as part of their job descriptions, one-size-fits-all cybersecurity training lacks relevance.

In many cases, companies have inconsistent policies around which systems employees can access, how sensitive data should be accessed and protected while working remotely, and whether employees can procure their own technology assets without cyber screening and sign-off from both technology and cybersecurity leaders.



**Key message for the business:** Senior business leaders can reinforce a culture of cybersecurity through regular communications stressing that protecting the business is the responsibility of every employee, no matter where they fall in the corporate hierarchy.

*[For more, see "Establish a culture of cybersecurity," page 14.]*

4

**Cross-institutional data sharing**

If it wasn't clear already, the pandemic shed light on the value of cross-institutional data sharing and collaboration on time-sensitive and complicated health issues. One company sharing information with another properly vetted company may not seem particularly risky. However, with multiple stakeholders and hyperconnected digital systems, companies don't have complete ownership of their data once it is shared outside of their organizations. This could create a significant theft risk for personal health information (PHI), which is, according to current estimates, significantly more valuable on the black market than financial data.<sup>1</sup>

While it may seem as if data are transmitted in a straightforward flow, the process is quite complex when you look more closely at the exchange points. For example, pharma companies need to coordinate simultaneous data sharing across various entities, such as individual states for order fulfillment; doctors' offices, long-term care facilities, schools, prisons, pharmacies, etc. in relation to immunization programs; government agencies to solidify drug pricing, and much more.



**Key message for the business:** Although industrywide collaboration is extremely valuable in terms of preventing, treating, and curing rare and emergent diseases, the free flow of data can put patient privacy at risk. Therefore, organizations must carefully assess how to strike a balance between the clinical value of strategic information sharing on the one hand and maintaining data privacy and avoiding compliance penalties on the other.

*[For more, see "Strike a balance between mining data for value and protecting patient privacy," page 15.]*

<sup>1</sup> M. Yao, "Your Electronic Medical Records Could Be Worth \$1000s to Hackers," *Forbes*, 2017.





5

**Neglecting to incorporate physical security into cybersecurity**

Although the convergence of physical and cyber threats is not new, the need for CISOs to coordinate physical security and cybersecurity was heightened during the pandemic. Of course, the surge in hybrid and remote work increases the risk of physical theft of computer devices, data, and more. However, there are also some very specific physical risks surrounding COVID-19 vaccine distribution.

In the U.S., military generals ensure the physical security of vaccines by guarding manufacturing plants, encrypted hard drives are transported by federal marshals to the FDA, and the National Guard escorts some vaccine shipments.

Some foreign governments require engagement with local law enforcement, negotiations with organizations like the European Medical Agency (EMA) on how to encrypt files, and consultation with local regulatory experts to ensure that pharma organizations comply with international regulations such as EU MDR and those related to doing business with government entities.



**Key message for the business:** At the same time as the number of cybersecurity concerns continues to proliferate, threat actors are increasingly launching physical attacks designed to prevent drugs and related data from getting to their intended endpoints. To avoid serious financial, reputational, and regulatory harm, organizations need to increase their investments in physical security measures as part of their overall security planning.

*[For more, see "Incorporate physical security into cybersecurity," page 15.]*

6

**Disinformation campaigns**

With respect to COVID-19 vaccines and treatments, CISOs face a new threat in the form of a massive disinformation campaign around efficacy, safety, side effects, the comprehensiveness of R&D, testing, and agency review, etc. From domestic groups to state-sponsored foreign actors trying to undermine U.S. vaccination programs, there is a seemingly endless flow of disinformation propagated via websites and social media. Spreading false or alarmist information about vaccines may not be new, but we are now seeing this phenomenon reach a massive scale.

With less weighty situations than the pandemic, false assertions are often limited to one person or one group, so they don't rise to the level of a threat. During the pandemic, unchecked disinformation raises a public safety risk as fears are stoked about the efficacy of vaccines and treatments. Further, if individuals turn to off-label use of drugs, they could have a false sense of safety, or worse, severely impact their health. Intangible attacks like disinformation campaigns are particularly insidious as, unlike more typical security-related attacks, they don't require technical skills and can be perpetrated by anybody.



**Key message for the business:** Since disinformation isn't weeded out from content posted on most social media platforms and websites, the onus is on pharmaceutical organizations to counter irresponsible and inflammatory claims related to their products.

*[For more see "Push back against disinformation," page 15.]*











DISCLOSURE IS NOT LIMITED



# Key cybersecurity principles for countering the top six threats

**The knowledge that global pharmaceutical companies have become more of a target than in the past is driving CISOs' conversations with the business about enhancing the security of their supply chain processes. These conversations are key to securing additional investments in talent, skillset development, and strategic partnerships across the cybersecurity landscape.**

As CISOs work with the business to pinpoint priority cybersecurity investments, the following are key principles to keep in mind:

-  1. Hold third parties to a higher standard
-  2. Focus on protecting the "crown jewels"
-  3. Foster a culture of cybersecurity
-  4. Strike a balance between mining data for value and protecting patient privacy
-  5. Incorporate physical security into cybersecurity
-  6. Push back against disinformation



DISCLOSURE IS NOT LIMITED



During the pandemic, there were peaks and valleys of cybercrime activity. At the beginning it was quiet. Things shifted when the crisis hit U.S. hospitals, then there was another peak when vaccine distribution occurred. The pandemic was a crisis for the healthcare industry. So, by ensuring that all aspects of the supply chain were as secure as possible, the cybersecurity community helped minimize disruption during this global health crisis.



—Lori Havlovitz  
CISO, Cardinal Health

### 1. Hold third parties to a higher standard

Pharmaceutical companies' cybersecurity efforts are complicated by the fact that additional risks can be introduced by third-party suppliers. In the effort to manage this seemingly intractable problem, CISOs and their teams can:

- **Codify** third-party risk management programs that specify the controls, systems, platforms, and security protocols partners and approved suppliers need to have in place.
- **Incentivize** suppliers to allow assessment of their cybersecurity programs for alignment with your internal security framework.
- **Refresh** incident response (IR) plans in case ransomware or viruses are introduced to your internal systems via third-party software applications.
- **Focus** on priority suppliers that sell raw materials, substrates, etc. for vaccines, and biologics, as well as regularly used products such as masks, pain medications, saline, etc.
- **Create** a centralized education and communication forum for your partners and suppliers.

### 2. Focus on protecting the "crown jewels"

As pharmaceutical organizations digitalize their operations, they must make a tradeoff between increased productivity and increased vulnerability. In a digital environment, companies can't protect all their assets with equal rigor. Therefore, it is imperative to focus on the assets where a breach could cause the most financial or reputational harm, or, worse, put patients at risk.

"The reality is, we can't protect everything," says Marene Allison of J&J. "You have to focus your efforts on protecting your crown jewels." To zero in on the most important assets, CISOs must:

- **Know** the ecosystem, i.e., who and what comprise the organization's supply chain.
- **Evaluate** how the configuration of the organization's central infrastructure contributes to the risk of cyber attack.
- **Prioritize** your assets by focusing the most robust cybersecurity protocols on systems that are difficult to bring back online.
- **Segregate** assets that you can afford to be without for a few days or even a few weeks, as well as legacy systems that may not be worth protecting due to their age.
- **Understand** that some functions that were less important before the pandemic may have become critical, e.g., call centers.





**3. Foster a culture of cybersecurity**

Everyone in the organization, from the most junior-level employee to the C-suite and the Board should understand that cybersecurity is not an IT issue as much as a people and process issue. CISOs play a critical role in establishing a culture of cybersecurity. As such, their purview should include empowering employees at all levels to take action; ensuring that the importance of cybersecurity is supported and evangelized by the senior leadership team; working closely with the communications team; and, in many cases, establishing new roles to help align the concerns of disparate groups.

*Empower employees*

- **Educate** employees on how to escalate to the appropriate company contact before taking actions that fall into a gray area in terms of cybersecurity.
- **Consider** allowing employees to unilaterally cut ties with suppliers that violate the firm’s security standards.
- **Conduct** tabletop cyber simulations that encompass not only the IT side of operations, but also OT and third-party suppliers and partners.

*Engage senior executives*

- **Provide** messaging to senior management to support employee communications about firmwide cybersecurity priorities and protocols.
- **Update** the executive operating team and Board on emerging threats on a regular basis, as this will likely drive funding and resources.
- Align business information security officers (BISOs) with business representatives to discuss and prioritize risks to vital business processes.

- **Check in** regularly with key stakeholders to ensure you are meeting with them on the right cadence.
- **Facilitate** executive visits to the shop floor so they can gain a clear view of how secure the organization really is.
- **Ensure** that C-level executives know what their roles entail in the event of an incident.

*Collaborate with communications*

- **Craft** “Cybersecurity 101” communications for members of non-technical groups who may not understand terms like threat monitoring, third-party risk management, etc.
- **Tailor** messaging to the business function you are addressing, e.g., HR, marketing, legal, finance, etc.
- **Provide** hands-on experiences to make highly complex ideas more accessible.
- **Understand** the communications protocols of business process outsourcing (BPO) vendors, e.g., how they plan to communicate with you during a crisis and who will communicate with the public.

*Establish roles that serve as liaisons between groups*

- **Expand** the cybersecurity team’s “brand” by including BISOs, threat intelligence groups, and other specialty roles.
- **Appoint** an OT business process champion to act as a single point of contact for OT cybersecurity.
- **Appeal** to the business functions to be cybersecurity advocates and evangelists in their divisions.



**Like many organizations, shifting to a predominantly remote workforce during the pandemic introduced new cybersecurity challenges and new solutions. Our enhanced infrastructure enables a new way of working while simultaneously addressing cybersecurity threats that emerged and were heightened as a result of the pandemic.**



— **Michael McNeil**  
Senior Vice President and Global CISO, McKesson







#### 4. Strike a balance between mining data for value and protecting patient privacy

There is no doubt that data is one of the most valuable assets pharmaceutical companies hold today. From analyzing patient data as the basis for new treatments and cures for chronic conditions to mining claims data to understand geographical and demographic disease patterns, the free flow of information is critical to patient care. On the other hand, the act of sharing data outside of an organization's four walls is fraught with patient privacy risks. Therefore, organizations must find the sweet spot between getting value from data and keeping PHI secure. To this end, CISOs can:

- **Establish** a detailed network diagram that provides visibility into the data flows permitted into, out of, and within both the IT and the OT environment.
- **Ensure** that the front of a system doesn't become an entry point to the entire system by instituting attribute-based access controls (ABAC).
- **Extend** access management policies to include remote access and third-party access, with a minimum requirement of multifactor authentication through a firewall.
- **Stay current** on existing and impending data privacy regulations and how they may impact the use of data in the manufacturing environment.

#### 5. Incorporate physical security into cybersecurity

At present, distribution and factory spaces have made progress on coordinating cyber and physical security considerations. CISOs can help extend that mindset to the entire pharmaceutical supply chain by taking care to:

- **Facilitate** frequent collaboration between cyber and physical teams so that both sides are up to date on evolving threats and vulnerabilities of mutual concern and can develop a joint IR plan with clearly defined roles and responsibilities.
- **Enhance** logistics security so final finished products make it safely and without tampering to wholesalers, distributors, hospitals, and patients.
- **Protect** peripheral materials, such as cardboard boxes, dry ice, facility banners, etc.
- **Remember** that executive protection should address both physical and cyber threats.
- **Adhere** to more stringent cybersecurity requirements and certifications when doing business with the U.S. government, particularly the Department of Defense.
- **Establish** working relationships with CISA, the National Cybersecurity Center of Excellence, and other cyber-hygiene organizations.

#### 6. Push back against disinformation

As COVID-19 vaccination rates vary on a state-by-state basis,<sup>2</sup> pharmaceutical firms and their cybersecurity organizations need to continue to counter disinformation campaigns by taking steps to:

- **Collaborate** with the federal and state governments to create public education campaigns and increase accessibility to vaccination centers.
- **Tap into** communications to identify trending key word searches and consider a public information ad campaign to run alongside top search results.<sup>3</sup>
- **Form** a consortium or other joint effort with other pharmaceutical CISOs to provide a united front on vaccine efficacy and safety.

<sup>2</sup> Katie Adams, "States ranked by percentage of population fully vaccinated," *Becker's Hospital Review*, October 18, 2021.

<sup>3</sup> "Information Campaigns and COVID-19 Vaccine Messaging: Applying Lessons Learned from the 2020 Election," National Governors' Association, August 3, 2021.





# Conclusion

**Clearly, the pharmaceutical industry has entered a new era of cross-institutional collaboration and mutual concern. From working with third-party suppliers and partners on their cybersecurity postures to collaborating on treatments and vaccines in the battle against COVID-19 and future global health crises, there is no doubt that toppling silos only makes the industry stronger.**

And of course, this paper and the accompanying practitioners' guide are cases in point. The hope is that the framework we have developed will be a work in progress and that other members of the Health-ISAC community—and the pharmaceutical industry at large—will weigh in as the pharmaceutical ecosystem evolves.

In the name of collaboration, pharmaceutical CISO organizations may want to pursue the following:

- Through organizations like Health-ISAC, make a commitment to share best practices and other information with peers and partners to help protect the ecosystem.
- Establish a set of industrywide cybersecurity protocols to which all companies will adhere.
- Have conversations with CISOs at other manufacturers and/or distributors about how to collaborate on protecting the supply chain.
- Commit to cross-organizational information sharing to promote situational awareness of threat actors; their motivations; campaigns; and tactics, techniques & procedures (TTPs).
- Coordinate efforts to stay abreast of software vulnerability disclosures and their potential impact(s) on organizations or the supply chain.
- Appeal jointly to suppliers to raise their cybersecurity postures, including putting contracts on the line if met with significant resistance.
- Work within the auspices of Health-ISAC to create a directory of domestic and foreign law enforcement agencies that can help with physical security.
- Support Health-ISAC in becoming a clearinghouse for information that can help facilitate collaborative cybersecurity efforts among companies.





DISCLOSURE IS NOT LIMITED



# Participating CISOs



## Marene Allison

**CISO, Johnson & Johnson**

Marene is responsible for protecting the J&J's Information Technology systems and data worldwide through elimination and mitigation of cybersecurity risk. This includes ensuring that the J&J information security posture supports business growth objectives, protects public trust in the J&J brand, and meets legal/regulatory requirements. With 265 companies in 60+ countries, J&J is a leader in consumer health, medical devices, and pharmaceutical products worldwide.



## Brian Cincera

**Senior Vice President and CISO, Pfizer**

Brian has global responsibility for Pfizer's information security and technology risk management program. In his role, Brian oversees strategy development, cybersecurity risk management, policy and governance, protection operations, and workforce awareness. As part of Pfizer's company-wide enterprise risk management program, Brian is responsible for leading its information security risk governance process including regular reporting to Pfizer's executive leadership and members of its Board of Directors. Brian joined Pfizer in 2005 and works in Collegeville, PA.



## Meredith Harper

**Vice President and CISO, Eli Lilly and Company**

As Vice President and Chief Information Security Officer at Lilly, Harper is responsible for the company's global information security program. Prior to joining Lilly in 2018 as Senior Director, Deputy Chief Information Security Officer, she served as Chief Information Privacy and Security Officer at Henry Ford Health System, where she had ultimate responsibility for the protection of Henry Ford's provider, insurance, retail, and research businesses. She holds a master's degree in health services administration and a bachelor's degree in computer information systems from the University of Detroit Mercy. She also earned a master of jurisprudence degree in health law from Loyola University Chicago School of Law. Harper serves on several advisory boards in support of empowering women and minorities to embark upon careers in technology, especially in information security.

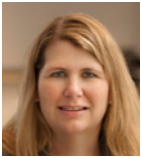


DISCLOSURE IS NOT LIMITED

Securing the modern pharmaceutical supply chain 17



**DISCLOSURE IS NOT LIMITED**



## Lori Havlovitz

**CISO, Cardinal Health**

Lori leads the global Information Security team at Cardinal Health which includes Cybersecurity Operations, Information Security Architecture, Technology Risk Management, IT Compliance, and IT Resiliency. While at Cardinal Health, Lori has held roles of increasing responsibility in Applications Development and Shared Services as well as Enterprise Architecture. Lori has been with Cardinal Health for 20 years. Before joining the organization, Lori worked with Nationwide Insurance focusing on system integration project management in the property and casualty business. She has held a variety of roles including chairing the Women's Initiative Network and an executive sponsor for the Women in Information Technology employee led group at Cardinal Health. She holds a BSBA in MIS/Finance from The Ohio State University and an MBA from the University of Dayton.



## Michael McNeil

**Senior Vice President and Global CISO, McKesson**

Michael is responsible for enhancing and overseeing McKesson's information and operational technology security strategy program, as well managing information security governance. He will also ensure the execution of McKesson's cybersecurity strategy across the enterprise. McNeil has an extensive background in cybersecurity and significant experience in the healthcare industry. Most recently, he served as the Global Product & Security Officer for Royal Philips where he deployed consistent processes across the entire portfolio of healthcare products and services. He has also held senior leadership positions at Medtronic, Liberty Mutual Group, Pitney Bowes, and Reynolds & Reynolds. Michael holds an MBA from Northwestern University, J.L. Kellogg Graduate School of Management and a Bachelor of Science Degree from the University of Illinois.

*We would also like to thank the following individuals for their invaluable input:*

### **KPMG**

**Mitushi Pitti**  
Director, KPMG

**Brad Raiford**  
Director, KPMG

**Donna Ceparano**  
Director, KPMG

**John Hodson**  
Director, KPMG

**Kristy Hornland**  
Manager, KPMG

**Daniel Christman**  
Associate, KPMG

**Haylee Thompson**  
Associate, KPMG

### **Pfizer**

**Dave Williams**  
Director, OT/ICS Security, Pfizer

### **McKesson**

**Edwin Drayden**  
Sr. Director, Information Security  
and Risk Management, McKesson

**Katie Ewers**  
Director of Cybersecurity, BISO  
Team, McKesson

### **Cardinal Health**

**Caitlin Kiska**  
Information Security Engineer,  
Cardinal Health

**Jessica McMeans**  
Information Security and Risk  
Engineer, Cardinal Health

### **Eli Lilly and Company**

**Jane Harper**  
Sr. Director Information Security  
Risk – Business Engagement, Eli  
Lilly and Company

### **Abbott**

**Fumi Collier**  
Director – Cybersecurity Services,  
Abbott



**DISCLOSURE IS NOT LIMITED**



DISCLOSURE IS NOT LIMITED



# Contributors



**Mike Wagner**  
Sr. Director, Information  
Security, Global Supply Chain,  
Johnson & Johnson



**Jonathan Dambrot**  
Principal, KPMG



**Sarat Mynampati**  
Principal, KPMG



DISCLOSURE IS NOT LIMITED



**DISCLOSURE IS NOT LIMITED**

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

[kpmg.com/socialmedia](https://kpmg.com/socialmedia)



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2021 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in the U.S.A. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. NDP258228-1A



**DISCLOSURE IS NOT LIMITED**