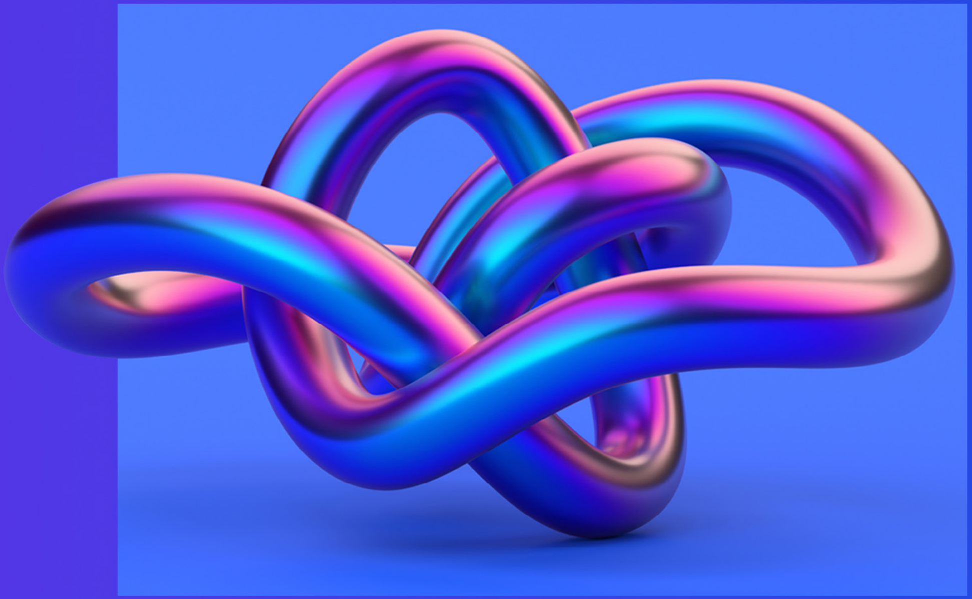
Cybersecurity considerations 2023

Life Sciences



Foreword

The CISO agenda is simple: protect intellectual property, clinical data, employee data, and the functioning of manufacturing sites. While the statement is not complicated, as a practical matter, it involves protecting a wide and ununiform attack surface.

IT is transforming as cloud, artificial intelligence/machine learning (AI/ML) engines, and ERP platforms continue to evolve. Today's technology is in a state of rapid transition and companies must contend with legacy systems used by businesses and manufacturing sites. This presents a complex challenge for CISOs that includes designing and securing the transformation, maintaining least privilege, managing the rise of AI, protecting patient data and IP, securing the supply chain, OT security, and maintaining compliance with global laws and regulations.

In addition to traditional security hygiene, such as patching, security training, backups, and risk assessments, many CISOs also are familiarizing themselves with and deploying a zero-trust agenda. Chiefly, this includes identity and access management to establish identity as an edge control and providing least privilege only after verifying the user's identity. Zero trust is not a software solution but rather a framework to secure various layers such as applications, data, end points, and networks with an architecture that authenticates and authorizes users before granting access.

For Life Sciences organizations, securing both the IT and OT environments and maintaining a mature and tested cyber resilience and response program are key to defending against malware and ransomware attacks in this ever-changing technology landscape. To effectively detect and respond to attacks, CISOs are constantly reducing the attack surface, building sensors, fine-tuning response plans, and testing preparedness. This strategy often requires a managed detection and response strategy and, at times, partnering with a managed services provider.

Finally, with advances in AI and ML, and the usage of these technologies in business processes such as clinical trials, securing these models has become latest CISO agenda item with automation now front and center in business transformation dialogues.

Chetan Gavankar

Principal,
Advisory Life Sciences, and
Cyber Security Lead, KPMG

Key cybersecurity considerations for Life Sciences in 2023

Click on each consideration to learn more.

01

Digital trust: A shared responsibility

Are organizations thinking broadly enough about how to protect the interests of employees, customers, suppliers, and partners?

02

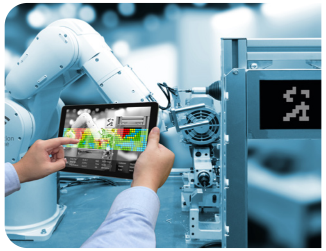
Unobtrusive security drives secure behaviors

How do security teams effectively integrate security into business processes, agile development programs, and disparate operating models?

03

Securing a perimeter-less and data-centric future

With the security perimeter all but gone, how can organizations pragmatically and realistically transition to a zero-trust approach that protects every aspect of their ecosystem?



04

Trust in automation

What can organization do to help ensure robotic process automation (RPA), machine learning (ML), and other forms of artificial intelligence (AI) are implemented and managed effectively, sensibly, and securely?

Consideration 1

Digital trust: A shared responsibility

Digital trust is finding its way onto board agendas as privacy, security, and ethics debates gain momentum—partly driven by regulation and partly by public opinion. The future success of any digitally enabled business is built on digital trust—cybersecurity and privacy are vital foundations for that trust. CISOs must be prepared to help the board and C-suite create and maintain the trust of their stakeholders if they are to create a competitive advantage. Realizing this potential requires a collective commitment from all stakeholders.

Globalization has made the world borderless and interconnected—a reality made only too evident by the disruption to global supply chains brought on by the pandemic. To create lasting relationships with customers (whether B2B or B2C), organizations must establish and maintain digital trust.

Value and trust

Trust is key to success—and is not just about reputation. Boosting trust can create competitive advantage and can add to the bottom line.

More than 1/3 of organizations recognize that increased trust leads to improved profitability.

But 65% report that information security requirements are shaped by compliance needs rather than long-term strategic ambitions.

65% of executives continue to view information security as a risk reduction activity rather than a business enabler.

49% believe that the board of directors sees security as a necessary cost rather than a way to gain competitive advantage.

Source: KPMG Cyber trust insights 2022.

Businesses are starting to care

Growing numbers of senior leaders recognize the benefits of digital trust, with 37 percent seeing improved profitability as the top commercial advantage of increased trust.[1] Digital trust encompasses a wide range of disciplines. Cybersecurity is a major part of that broad spectrum of closely linked digital trust–related issues—reliability, safety, privacy, and transparency. These areas impact how companies conduct business and pursue values; the products and services provided; the technology used; how to collect and use data; and how to protect the interests of customers, employees, suppliers, and all other third-party partners and stakeholders.

By contrast, 65 percent continue to view information security as a risk reduction activity rather than a business enabler.[2] Many organizations still view cybersecurity primarily as a cost and not necessarily as an investment in the future, which is misguided. CISOs should embrace the concept of digital trust and demonstrate how security as an enabler for the business will securely support an organization's digital growth agenda.

CISOs have a significant role in helping their organizations build digital trust, but they cannot do it alone. They should invest sufficient time in encouraging other critical internal and external stakeholders with respect to their respective roles on the digital trust journey. Indeed, CISOs must demonstrate to the C-suite and board why this is such an important topic and how digital trust depends on clearly articulated, business-focused strategies.

As the World Economic Forum (WEF) suggests, companies are beginning to acknowledge that cybersecurity is as much a strategic business element as enterprise risk, product development, and data management. In its report, Earning Digital Trust: Decision-Making for Trustworthy Technologies, the WEF writes, "digital trust requires a holistic approach, where cybersecurity is one dimension of trust among many."[3]

What digital trust means to customers

While the typical retail consumer may not care about the nuts and bolts of a company's formal data protection program, the moment customers learn of a breach, they want to know what action is being taken and that their interests are at the heart of the response. The organization can reestablish trust over time by responding to the incident expeditiously and transparently.

Today's consumers understand that breaches happen, and gradually, most come back if the company offers solid products and services at a competitive price point, there is a consistently positive customer experience, and the details around the response to and recovery from a cyber event are clearly communicated and reassuring.

[1] KPMG International, KPMG Cyber trust insights survey, "Building trust through cybersecurity and privacy," 2022.
[2] Ibid.
[3] World Economic Forum, Earning Digital Trust: Decision—Making for Trustworthy Technologies," November 2022.

Digital trust strategies that work

It's vital to embed the concept of digital trust into corporate strategy, product development, and the company's overall market presence and relationship with corporate and retail customers. Thinking broadly about what digital trust means across different stakeholder groups can help underline the importance of cybersecurity and the other disciplines that contribute to establishing and maintaining digital trust, as well as encourage a holistic approach across disciplines.

Trust is a function of specific technologies developed or deployed, and the decisions leadership makes. CISOs must continually support a narrative for the board and C-suite to clarify why and how cybersecurity is an integral building block for digital trust.

CISOs must help drive decisions around the right partners and suppliers. Qualifying criteria must be established covering transparency regarding information protection practices and the organization's ability to demonstrate adequate recovery and response resilience.

Make no mistake, regulatory obligations are expected to grow regarding the components of digital trust, and so can expectations over the levels of transparency and accountability regulators expect from companies in this regard. A principle-based and holistic approach to meeting the diverse and increasingly complex regulatory landscape can pay dividends and avoid creating costly compliance-driven silos.

It starts at the top and filters down—if leadership accepts and lives this narrative, so should the rest of the organization. That means making it a tangible feature of the company's annual report, in which the company's philosophy and strategy around digital trust by design are outlined in detail. With 34 percent of corporate leaders concerned about their businesses' ability to satisfy reporting requirements for greater transparency over cybersecurity and privacy, KPMG professionals advocate a proactive approach.[4]

Life Sciences considerations

Transparency means different things to different audiences. Simply put, life sciences companies that are able to establish trust among all stakeholders, including customers, in their products and services—specifically in how they operate and protect the business and customer data—are more likely to see positive commercial and reputational impacts.

Everyone has responsibility in building and sustaining digital trust. CISOs and their teams must demonstrate their commitment to the board and build the narrative around cyber as an enabler of trust and, in turn, competitive advantage. There's responsibility and actions to be taken at every level to ensure there is a shared understanding of what digital trust truly means and the operational, business, and board levels.

Security protects not only the firm's interests, but also the interests of our customers and partners. And it impacts all those stakeholders in various ways. It's critical, if companies are to achieve digital trust, to embed security and resilience into corporate strategy, product innovation, customer experience, and service.

[4] KPMG Cyber trust insights survey. Op cit.

Consideration 2

Unobtrusive security drives secure behaviors

Embedding security within the business in a way that helps people work confidently, making productive choices, and playing their part in protecting the organization must be a key, albeit often elusive, CISO objective. It's all too easy for people to see security as an impediment, and only by considering security from both human and business-centric perspectives can CISOs hope to change this mindset.

Perhaps the most essential point is to be attentive to where and when security matters most and where additional security measures will likely impact the business justifiably. There is no absolute security, and if CISOs try to protect everything at every moment, they risk protecting nothing as users find ways around intrusive security measures. CISOs need to be pragmatic around the extent of security controls that are warranted and commensurate with the criticality of the specific business process and the related risk profile.

Confidence in the CISO

Organizations display high levels of confidence and strong belief in the CISO's ability to deliver on crucial tasks.

79% of organizations are confident CISOs can accurately map where critical data is across the enterprise.

3/4 are confident CISOs can identify what their crown data jewels are.

78% are confident CISOs know how much of their sensitive data is with third parties and that it's appropriately secured.

Source: KPMG Cyber trust insights 2022.

Companies should move away from thinking about enterprise security in binary terms. In today's environment, it's a moving target, and the concept of "secure" versus "not secure" is transitory. Instead, CISOs should work to raise the organizational IQ around cybersecurity through awareness; simple, intuitive processes engineered with users in mind; and a better-informed employee base and executive team.

Customer experience applies to security too

It's crucial to focus on building realistic processes for responsible users while still having the means to detect and quickly counter malicious activity. It boils down to ease of use, customer experience, and planning around cybersecurity within the context of enterprise-wide priorities—the commercial needs of the broader business—as opposed to thinking of it purely as a regulatory imperative.

Advances in technology can help. From defensive AI, machine learning, and chatbots to cloud encryption, blockchain, and extended detection and response applications, all are vital parts of the puzzle. So too is creating a more security-aware workforce, guided by consistent IT governance, to inspire people to approach digital communications with appropriate caution. CISOs should consider how they can help employees do the right thing instinctively and design security controls that support them in doing so.

As an ongoing, ever-evolving endeavor, cybersecurity presents many opportunities to "bolt-on" new tools and controls. Still, we encourage organizations to build it in from the beginning, considering the human element. Major transformational initiatives have many components—one should be security. Building security into broad process-oriented initiatives, such as DevSecOps, operational technology, and procurement, can be an effective and unobtrusive way to motivate people to behave securely and function as human firewalls without seeming overbearing.

Security teams can learn much from the way organizations enhance the customer experience. Internal security controls should be easy to use, or employees may be motivated to bypass these processes; consider including customer experience specialists in the design of controls.

Security processes should also be personal for internal users. Require the individual to make judgment calls, explain the context, draw a parallel between the value of cautious, secure behavior in their personal and professional lives, and make them "edutaining." People can then play their part in the security and not be seen as the weakest link.

Life Sciences considerations

Security is a fluid journey—the scenery is always changing as we move further. Simply put, organizations that prioritize security as a top strategy are more likely to protect their patient data, as well as their own intellectual property, than those that do not.

Life sciences companies, such as firms in other critical industries, need to accept that technology will not, in and of itself, solve the security problem. Indeed, huge capital flow into cybersecurity. There are thousands upon thousands of cybersecurity companies in the market with tools designed to address numerous challenges. And yet, we seem to be as vulnerable as ever. Because the bad actors also have access to these tools.

Companies should acknowledge that a more security-aware workforce will likely move the needle much more efficiently than just the tools by themselves can. Clearly, today's sophisticated security tools are essential, but it starts with an alert workforce and CISOs, and their teams can be instrumental in embedding a robust cybersecurity culture across the enterprise.

Additionally, life sciences firms should ensure that they are participating in the right forums, industry discussions, and ISACs (Information Sharing and Analysis Centers). This outreach will make companies more aware from an outside-in perspective and create partnerships that can drive new, forward-looking insights.

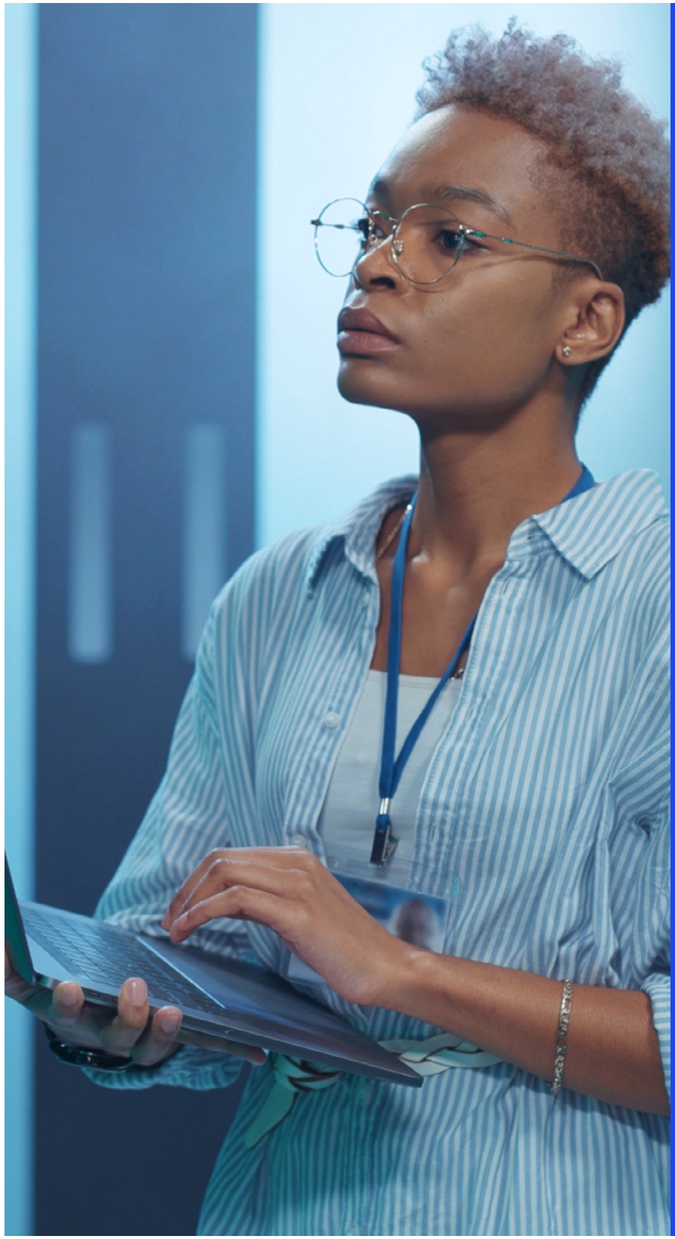
In the end, it is essential to align the overarching cybersecurity program with the firm's broader business objectives. If you think of cybersecurity solely in terms of protection, and not also as a business enabler, your investments are likely to underperform. Companies are encouraged to think of it as a necessary building block for profitability and trust.

Consideration 3

Securing a perimeterless and data-centric future

It's no surprise that business operating models have fundamentally changed over the last decade—becoming more fluid, data-centric, connected ecosystems of internal and external partners and service providers. In this distributed computing world, to help reduce the blast radius of any potential outages or breaches, CISOs and security teams must adopt very different approaches, such as zero trust, Secure Access Service Edge (SASE), and cybersecurity mesh models.

Today, the clear business imperative is to enable employees, customers, suppliers, and other third parties to connect seamlessly, remotely, and securely. The accompanying security challenge is that, in a perimeter-less environment, organizations are no longer able to trust every user and device.



Data security is a key issue for stakeholders

In a perimeter-less environment, concerns over how data is protected, used, and shared are the leading factors undermining stakeholders' trust in an organization's ability to use and manage its data.

28% of executives identify "a lack of confidence in the governance mechanisms in place" as a leading factor undermining stakeholders' trust in an organization's ability to use and manage its data.

32% also identify "a lack of clarity over why data is required for a particular service and the benefits of sharing or providing data" as another factor.

36% are concerned over how their data is protected.

35% are concerned over how their data is used or shared.

Source: KPMG Cyber trust insights 2022.

Zero trust for perimeter-less businesses

Zero-trust approaches can help reduce the blast radius in the event of an outage or breach and limit the impact so the incident can be better managed and contained. SASE and cybersecurity mesh models with a foundation in zero trust have common principles in terms of how security overall is organized, distributed, and aligned across the network. Perhaps most important, however, is that as more enterprises adopt a cloud-centric mindset, it has become critical to move security mechanisms closer to the data.

As an umbrella over today's perimeter-less business environment, zero trust is a framework, a way of thinking about how the design and enablement of security and identity access need to change over time. Zero trust complements the convergence of services under a SASE model and the holistic, analytical cybersecurity mesh architecture.

Life sciences considerations

In a perimeter-less environment, zero trust should be defined in relation to every scenario, every user, and every end point—representing a key pillar of the company's foundational security program. Life sciences CISOs must play a key role not only in codifying the zero-trust model and message, but also in establishing policies, setting standards, designing software solutions, and assembling an enterprise-wide security council encompassing various technology and business leaders.

Another challenge is around funding and budgeting. CISOs must be able to explain the framework around zero trust, so the board and other corporate leaders understand that the investment is not just another new technology but a new way of thinking that is designed to support a secure, perimeter-less future.

Finding a middle ground between on-prem and off-prem structures should be a clear objective, particularly with cloud-native technologies. Indeed, many life sciences companies are looking at transitioning multiple processes to the cloud, but many legacy infrastructures cannot fully adapt to cloud's SASE (Secure Access Service Edge) specifications because of the advanced technology requirements.

CISOs at large, complex organizations have the challenge of managing a security posture that spans an on-prem or off-prem ecosystem that can result in higher operational costs in the short term while operating in this dual environment. Life sciences looking toward full cloud adoption should consider the same on-prem zero-trust principles for systems they deploy into the cloud. They should also factor in the impact of an operating model change. For example, a well-managed shared responsibility model with a cloud provider can be key to helping ensure a secure cloud architecture.

Consideration 4

Trust in automation

In the race to innovate and harness emerging technologies, concerns over security, privacy, data protection, and ethics, while gaining more attention, are often ignored or forgotten. Left unchecked, this negligence could lead businesses to sabotage their potential, especially with new AI privacy regulations on the horizon.

Historically, AI has been a series of data science experiments, with a relatively small percentage of projects going into production. Now, the age of applied, real-world ML has dawned, and over the next 18 to 24 months, you should expect to see more of those projects go live.

There's been much trial and error, but the learnings can ultimately lead to huge success in the form of recommendation engines, decision support tools, sophisticated simulations, and neural networks that may unlock hundreds of millions of dollars of value for many organizations.

Automating mundane, repetitive tasks frees time and creates efficiencies so workers can focus on initiatives requiring complex, deliberative, nuanced thought. Hence, AI is being used across many industries. In the banking sector, bots are helping to decide the most appropriate products and services for clients, and in insurance, the use of automated decision-making in an applicant's creditworthiness assessment is being explored.

Challenges of AI/ML

There are growing societal and business concerns over the ethics, security, and privacy implications of adopting AI and ML solutions for big data analysis.

78% agree that AI and ML bring unique cybersecurity challenges.

3 in 4 say AI and ML raise fundamental ethics questions.

76% of executives agree that AI/ML adoption requires additional safeguards around how AI/ML systems are trained and monitored.

76% agree that AI/ML adoption requires transparency in how we use AI/ML techniques.

Source: KPMG Cyber trust insights 2022.

Building trustworthy and credible AI models

Are companies utilizing AI appropriately and getting the most productive output? With the insurance use case, there are instances where the algorithm makes decisions about applicants who live in specific areas. Those who live in less affluent neighborhoods were rated differently than those who live in more upper-class neighborhoods. As a result, premiums would differ based on the applicant's address. AI bias can be viewed as discriminatory and needs to be reined in.

Historically, applications were developed to run uniformly—the relationship between the inputs and corresponding outputs was not supposed to change. That was what developers tested against. The end user decided if they liked using the application and whether or not they wanted to continue doing business with the developer.

ML and AI tools are designed to learn and evolve. And that evolution represents a massive transformation in how companies must now think about these systems, how they've been trained and their fit for purpose.

People have mixed feelings and understanding of AI. And many companies simply don't have many professionals who understand AI, let alone how to secure it.

Machines, such as DevOps, are beginning to assume a role in shortening the development lifecycle and ensuring continuous delivery. And if businesses don't bring security into that machine-powered environment, it may never achieve scale because people simply won't trust it. To that end, 76 percent of executives agree that AI/ML adoption requires additional safeguards around how AI/ML systems are trained and monitored.[5]

AI and data privacy

AI elevates many core privacy principles—empowering security teams to analyze customer data more deeply, for example—but organizations need to think about proportionality with respect to the amount of data they collect relative to the data minimization requirements in certain regulations. Similarly, considering AI has the potential to embed existing biases, there must be transparency around the output.

Regulators, governments, and industry must work together. AI regulation isn't just a privacy issue. It requires data scientists to work with privacy specialists to determine what requirements should be built into the technology to make it safe, trustworthy, and privacy sensitive. And governments need to set the tone and establish an overarching digital agenda to inspire the industry to put budget behind innovation.

While various government bodies sometimes seem to approach AI as a competition, regulators are also starting to try to limit intrusive and high-risk applications of emerging AI capabilities.

Following the G20 adoption of principles for trustworthy AI, there have been major developments in AI risk management and regulation. Singapore was fast off the mark with its AI security standard, the National Institute of Standards and Technology (NIST) has published its AI risk management framework, and the EU AI act will follow later in the year. Regulation in this space is expected to ultimately have an impact as significant as GDPR has had on privacy. Many companies need to prepare.

Life Sciences considerations

With enabling patient care as a primary objective, the ability to leverage algorithms that support pattern recognition within big data is a huge opportunity that aligns with the core business goals of Life Sciences companies. However, patient safety comes with a vital responsibility: security. From a security perspective, there are several keys to justified trust in AI and ML—the intersection of being both trusted and being worthy of trust—as highlighted below.

Companies should ensure they have visibility into where AI is being used across their organization, and that it has been documented sufficiently. Security of AI applications, from the discovery of new lifesaving solutions to augmentation of administrative activities—such as processing of sensitive data—should be embedded from inception and present throughout the model lifecycle.

Education and awareness among employees interacting with AI/ML models are also essential. This is especially relevant in the R&D and clinical spaces, where open-source knowledge sharing is common, and workers may not consider the intentional and malicious attacks that can exploit the unique vulnerabilities of AI relative to deterministic software development.

Life Sciences firms should also establish cross-functional steering committees that connect business, legal, privacy, security, user experience, IT, and R&D functions to ensure secure AI governance is embedded across the organization.

It is also critical for Life Sciences organizations to remain aware of cross-industry regulations such as the EU AI Act to which companies that operate internationally may be held accountable. There are also impending state laws and emerging industry-specific requests for information around AI governance, such as the March 2023 FDA request for information regarding AI in Drug Manufacturing.

[5] KPMG Cyber trust insights survey. Op cit.

Cyber strategies for 2023

What actions can CISOs and the broader business lines take in the year ahead to help ensure security is the organization's golden thread? The following is a short list of tangible steps CISOs should consider as they seek to accelerate recovery times; reduce the impact of incidents on employees, customers, and partners; and aim to ensure their security plans enable—rather than expose—the business.

People

- Prioritize a robust cybersecurity culture that is interesting, engaging, and, where appropriate, fun to inspire employees to do the right thing and function as human firewalls.
- Build a security team with the skills mix needed to manage a perimeter-less organization, including cloud and third-party dependencies.
- Communicate broadly and clearly. Ask leaders in other organizational functions about their pain points and how automated processes might help.
- Take a multidisciplinary, cross- culture approach. Establish a security ecosystem comprising internal business line specialists, security professionals, data scientists, privacy-oriented attorneys, and external policy and industry professionals.
- Embed yourself in the organization and act as a peer, a sounding board, and an adviser.

Process

- Build consistent approaches to cyber risk management with an understanding of threat scenarios and attack paths to help inform attack surface reduction and prioritize control improvements.
- Focus on fit-for-purpose security processes that feature consistent user experiences.
- Establish strict identity controls and work to achieve a mature state of identity governance and services.
- Segment legacy environments to limit the attack surface and help contain any breaches.
- Have a proactive recovery plan focusing on the organization's most critical workflows with a communication structure and stress test it often.
- Consider subscription support models with predictable costs, any-shore delivery, and strategic results.

Data and technology

- Embrace the inevitable automation of the security function—trust the latest tools, such as robotic processes; security orchestration, automation, and response (SOAR); and extended detection and response (XDR) systems.
- Work with cloud providers to help ensure broad visibility into how products and services are configured to avoid inadvertent vulnerabilities.
- Consider cybersecurity and privacy issues up front when exploring emerging technologies, including the evolving risks associated with adopting AI systems.
- Assign responsibilities and establish accountability around how critical data is processed and managed and how it supports critical business processes.
- In the interest of speed, scalability, and trust, a transition to identity as a service in the cloud needs to happen sooner than later.

Regulatory

- Be aware of changing regulatory trends and drivers and what they could mean for the company's future technology strategy, product development, and operations.
- Consider the regulatory impacts vis-à-vis AI and automation—establish a clear concept of what the business can and can't do in these arenas and be alive to public concerns and changing expectations.
- Explore automating compliance monitoring and reporting and task a team member to serve as a regulatory monitor to stay on top of privacy and security regulatory trends.
- Align security and privacy compliance strategy with the company's broad business strategy to help ensure stakeholders from across the organization are on the same page.
- Look beyond the letter of the regulation—and be prepared to ask yourself more fundamental questions about digital trust and how you make that central to your strategic thinking.

How KPMG professionals can help

KPMG firms have experience across the continuum—from the boardroom to the data center. In addition to assessing your cybersecurity and aligning it to your business priorities, KPMG professionals can help you develop advanced digital solutions, implement them, monitor ongoing risks, and help you respond effectively to cyber incidents. No matter where you are in your cybersecurity journey, KPMG firms can help you reach your destination.

As a leading provider and implementer of cybersecurity, KPMG professionals knows how to apply leading security practices and build new ones that are fit for purpose. Their progressive approach to cybersecurity also includes how they can deliver services, so no matter how you engage, you can expect to work with people who understand your business and your technology.

Whether you're entering a new market, launching products and services, or interacting with customers in a new way, KPMG professionals can help you anticipate tomorrow, move faster, and get an edge with secure and trusted technology. That's because they can bring an uncommon combination of technological experience, deep business knowledge, and creative professionals passionate about helping you protect and build stakeholder trust.

KPMG—the difference maker

Contact us

Chetan Gavankar
Principal and Life Sciences Leader
Cyber Security Services
KPMG in the US
T: 617-988-1471
E: cgavankar@kpmg.com

Steve Sapletal
Advisory Industry Leader,
Life Sciences
KPMG in the US
T: 612-708-2556
E: ssapletal@kpmg.com

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

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.