accentureconsulting

THE SCIENCE OF SECURITY

ACHIEVING CYBER RESILIENCE IN LIFE SCIENCES

Accenture Life Sciences

Patient Inspired. Outcomes Driven.

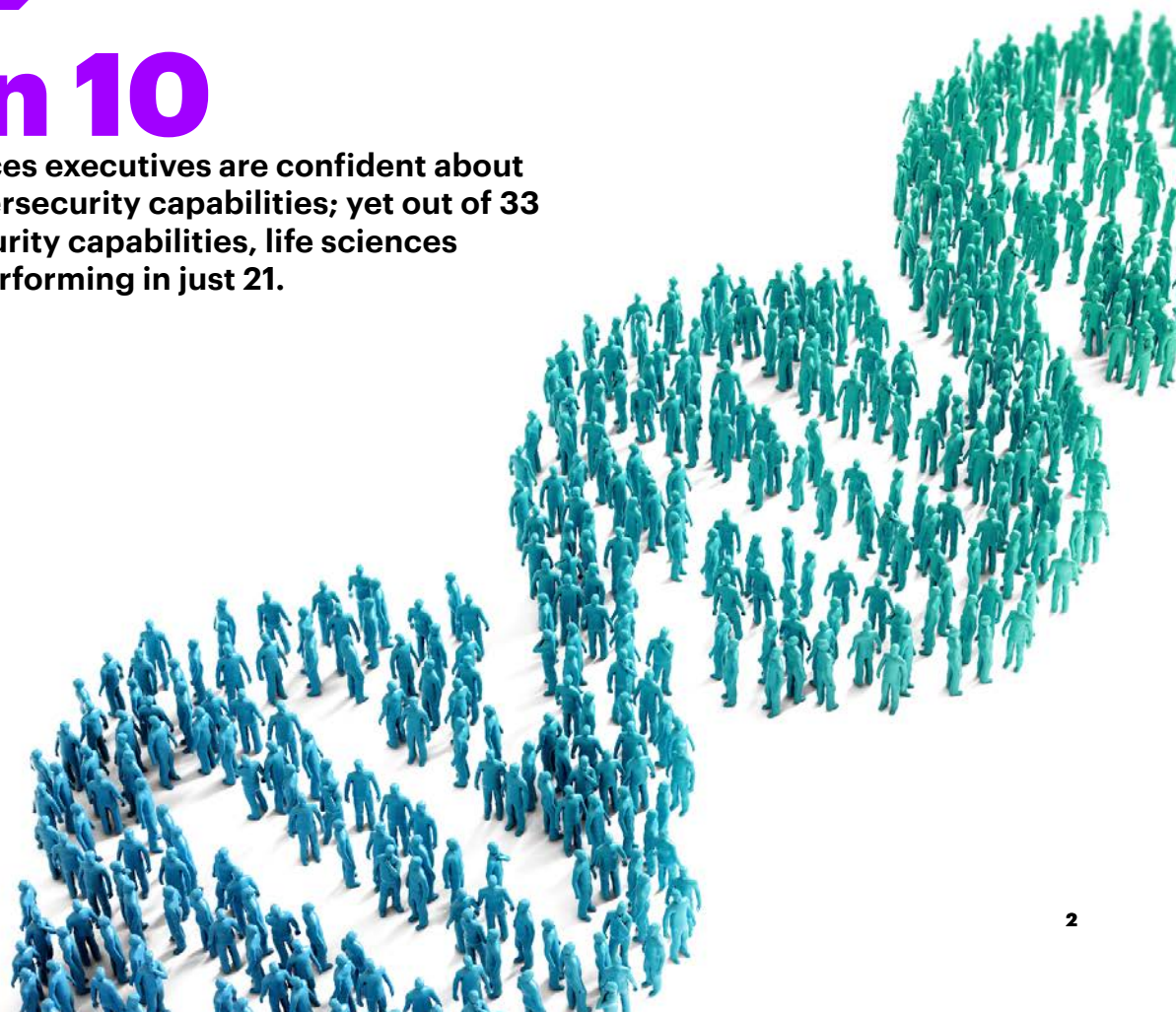
Security health

Increasingly, the success of life sciences companies is about their ability to deliver value through better patient outcomes. But while this shift creates infinite new possibilities to reinvent the patient experience and redefine the future of healthcare, it also introduces life sciences organizations to new security risks. Delivering better outcomes demands greater use of real-world evidence—more collaboration and data sharing across the healthcare ecosystem which, in turn, exposes vulnerabilities. Sixty-nine percent of life sciences organizations say their dependence on the Internet is growing and cybersecurity risks are also increasing. As fast as they shore up their defenses, new cyberattacks are evolving—with the potential to severely disrupt existing research and development (R&D), sales, marketing, medical affairs and manufacturing operations.

With dozens of companies hit by ransomware in recent years, and the average cost of cybercrime for an organization increasing 11 percent in 2018 over 2017,[1] life sciences organizations have yet to achieve cyber resilience.

8 in 10

life sciences executives are confident about their cybersecurity capabilities; yet out of 33 cybersecurity capabilities, life sciences is high-performing in just 21.



Security is not a one-time event

Life sciences executives must monitor and protect their businesses from pervasive threats as new risks open up in operational environments and supply chains. Security breaches affect life sciences organizations' profits, sales and even reputation—whether incurring data loss that results in regulatory fines, halting production, or negatively impacting brand or trust.

In addition, merger and acquisition (M&A) activity is, once again, on the rise in life sciences and with each announcement, the security challenge becomes more complicated—in an environment that is already known to be highly proprietary and complex. For an industry still bound to many legacy systems, defending them is expensive.

74% **of life sciences executives said that "cyberattacks are a bit of a black box, we do not quite know how or when they will affect our organization."**

Being able to prepare and recover effectively is essential when even robust cybersecurity strategies are proving vulnerable. Three areas are important for life sciences companies that want to achieve cyber resilience:

Drive business-enabled security

Protect beyond your four walls

Be brilliant at—and evolve—the basics

Drive business-enabled security

The scope of the CISO's role is evolving. Now, CISOs need to become the universal translator for cybersecurity—someone who is business-minded as well as tech-savvy. They must have a voice at the highest levels of the organization, so that they can align with and fully support the needs of the business—using terms with which the business is familiar.

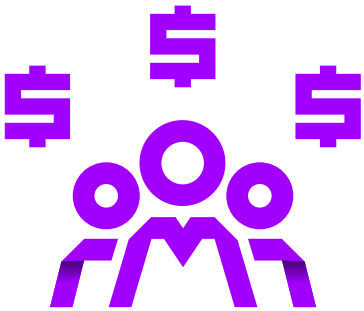
Our research found that the cybersecurity budget rests at highest levels of the life sciences organization—34 percent with the CEO or Executive Committee. Without a seat at the boardroom table, CISOs will struggle to deliver business-enabled security.

In our survey for the World Economic Forum in January 2019, we found that the Internet and Internet of Things play an essential role in the digital economy with the potential to generate US$642 billion across the whole of the life sciences industry over the next five years.[2] And 92 percent of life sciences business leaders said a trustworthy digital economy is critical to their organization's growth. CISO's are also in a vital position to secure digital trust—the key to drive future business growth and shared prosperity.

Cybersecurity budgets rest at the highest levels of the life sciences organization—

34%

with the CEO or Executive Committee.



Protect beyond your four walls

Digital technologies have created transformative disruption within many life sciences organizations. But while digitalization has enabled companies to enter more markets and grow, it also increases risk. Many IT departments have failed to keep up. And elements of the supply chain are often beyond an organization's direct control.

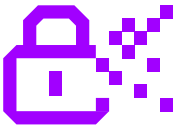
IT teams cannot afford to simply maintain the status quo. While traditionally life sciences organizations have focused their security efforts on enterprise systems, now they need to build new capabilities and operating models—with the security function acting as a business partner to enable growth, rather than a cost center. After all, decisions about growth and revenue are influenced by the whole business—from engineering and genetics, to laboratories, manufacturing and research and development. Also, they need to account for their entire ecosystem, not just their own four walls. In the Accenture Technology Vision 2019, only 19 percent of life sciences executives report that they know their ecosystem partners are working diligently, like they are, to be compliant and resilient with regard to security.[3]

As organizations develop their digital capabilities, they need to account for security growth. The impact of failing to address vulnerabilities should not be underestimated. Security leaders must employ an effective strategy and embed security within the business, while keeping an eye on the resilience necessary to serve the needs of tomorrow. Appropriate safeguards should also be extended as organizations modernize and embrace emerging technologies, such as artificial intelligence. In short, security needs to be there from the get-go. Embedding security into digital modernization programs, across the enterprise, is a necessary step in building cyber resilience.

87% of life sciences executives agree that, to be truly resilient, organizations must rethink their approach to security in a way that defends not just themselves, but their ecosystems.[4]

Safeguarding cloudification

A global biotech giant wanted to protect its massive cloud environment that centralizes highly sensitive patient, genomic and molecular data. Accenture helped to improve security in the cloud by introducing sophisticated identity and access management services and better data privacy controls. We also provided core security services, updating how they handled applications and cyber defense, and advised on security governance and compliance. And with huge efficiency gains, the company can now get life-saving treatments to people faster.



Be brilliant at—and evolve—the basics

Accenture research has shown that 32 percent of life sciences executives expect to significantly increase (double or more) investment in cybersecurity in the next three years. Yet their journey to cyber resilience is still some way off—out of 33 cybersecurity capabilities, life sciences is high-performing in just 21. Recovery from a cyberattack can be slow—85 percent of life sciences respondents said that, on average, it takes around 60 days to remediate a breach—a considerable 11 percent more than the global average.

With strong security foundations, such challenges can be managed. But life sciences executives recognize that they need to improve on the "basics" of cyber threats—50 percent identify security monitoring as most needed in their organizations to fill gaps in their cybersecurity program and 48 percent said network security is needed—both findings exceeding the global average (46 percent and 44 percent respectively).

To be prepared to monitor, react and bounce back, life sciences organizations must strive to become brilliant at the basics, identifying and protecting their high-value assets, prioritizing legacy applications and preparing for the worst by transforming their incident response plan into a crisis management plan.

But what constitutes the basics does not stand still. Just as cybercriminals are constantly adapting to find new security vulnerabilities, organizations must continuously evolve their security basics, leveraging new capabilities and the latest technologies, such as artificial intelligence. They should establish a new IT, making the best of new technologies and existing legacy data and services so that they can better serve patients and their business.

Act Now

No matter how well an organization has prepared for recovery, there is always a risk that things will not go to plan. But life sciences executives need not feel daunted. They can achieve cyber resilience by taking the following five actions:

1

Evolve the role of the CISO

There needs to be a new kind of CISO who is equally at home in the boardroom as the security operations center; someone who can transform the role to meet the needs of the intelligent enterprise.

2

Protect the value chain

When an attack occurs matters. Understanding the state of your clinical trials or manufacturing operations can help to focus your security efforts and prioritize your response to better manage business cycles.

3

Embed operational resiliency

With many attacks taking place out of business hours or on weekends, it is important to embed operational resiliency into everyday activities, no matter when they take place. Practice the recovery plan. Pressure-test resilience for greater speed and agility. Be prepared for a changing threat landscape.

4

Establish a robust recovery plan

Actively plan for the disaster that will happen by being brilliant at the basics; determine where your high-value assets are and direct your efforts there.

5

Adopt a data-driven approach using breakthrough technologies

Use artificial intelligence to see data patterns that go beyond human capabilities to seek out data anomalies. Use intelligence and data analytics to drive cyber resilience. Also, account for the additional risks that come from automation and non-human entities, such as chatbots.

Security first

Cyberattacks are often indiscriminate with different companies becoming collateral damage in what is often an unrelated war.

In fact, an organization does not need to be targeted by a hacker to experience tremendous loss—it may simply be "at the wrong place at the wrong time."

No matter the number of manufacturing facilities or whether a sound cybersecurity strategy has been embedded into a company's culture, the risk of an attack to patient and product data is looming. While life sciences executives know that they can rely on regulation to help guide how they operate, it cannot ease the complexities from these new threats. As key life sciences players have shown, cybersecurity is a priority—and the time to act is now.

82% **of life sciences executives think new technologies such as artificial intelligence (AI), machine or deep learning, blockchain and others are essential to securing the future of their organizations.**

Authors

Vikram Desai
Managing Director
Global Lead, Products Security
v.desai@accenture.com

Geoffrey Schmidt
Managing Director
Global Lead, Life Sciences Technology
geoffrey.d.schmidt@accenture.com

Cesar J. Villalta
Managing Director
Security, Life Sciences
cesar.j.villalta@accenture.com

Wayne Dennis
Senior Manager
Products Security
wayne.dennis@accenture.com

Stay Connected

@AccentureLifSci
@AccentureConsIt

/company/accenture_life_sciences
/showcase/accentureconsulting

accenture.com/lifesciencesblog

Notes

Unless otherwise stated, the statistics in this point of view represent life sciences respondents in the survey report "Gaining ground on the attacker: 2018 State of Cyber Resilience," Accenture.

References

[1] Ninth Annual Cost of Cybercrime Study, Accenture 2019. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

[2] Securing the Digital Economy, Accenture 2019. https://www.accenture.com/us-en/insights/cybersecurity/reinventing-the-internet-digital-economy

[3] Accenture Technology Vision 2019. https://www.accenture.com/us-en/insights/technology/technology-trends-2019

[4] Ibid.

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 477,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at **www.accenture.com**.

About Accenture Life Sciences

Accenture's Life Sciences group is committed to helping our clients make a meaningful impact on patients' lives by combining new science with leading edge technology to revolutionize how medical treatments are discovered, developed and delivered to people around the world. We provide end-to-end business services as well as individual strategy, consulting, digital, technology and operations projects around the globe in all strategic and functional areas—with a strong focus on R&D, Sales & Marketing, Patient Services and the Supply Chain.

We have decades of experiences working with the world's most successful companies to innovate and improve their performance across the entire Life Sciences value chain. Accenture's Life Sciences group connects more than 15,000 skilled professionals in over 50 countries who are personally committed to helping our clients achieve their business objectives and deliver better health and economic outcomes.

About the Research

In 2018, Accenture Security conducted the State of Cyber Resilience research—surveying 4,600 executives to understand the extent to which organizations prioritize security, how comprehensive their security plans are, what security capabilities they have, and their level of spend on security. Respondents represented organizations with annual revenues of US$1bn or more—from 19 industries and 15 countries across North and South America, Europe and Asia Pacific. More than 98 percent of respondents were sole or key decision-makers in cybersecurity strategy and spending for their organization. Of the 4,600 executives interviewed, 200 were in the life sciences industry across 11 different countries—Australia, Brazil, Canada, France, Germany, Ireland, Japan, Netherlands, Norway, UK, US.