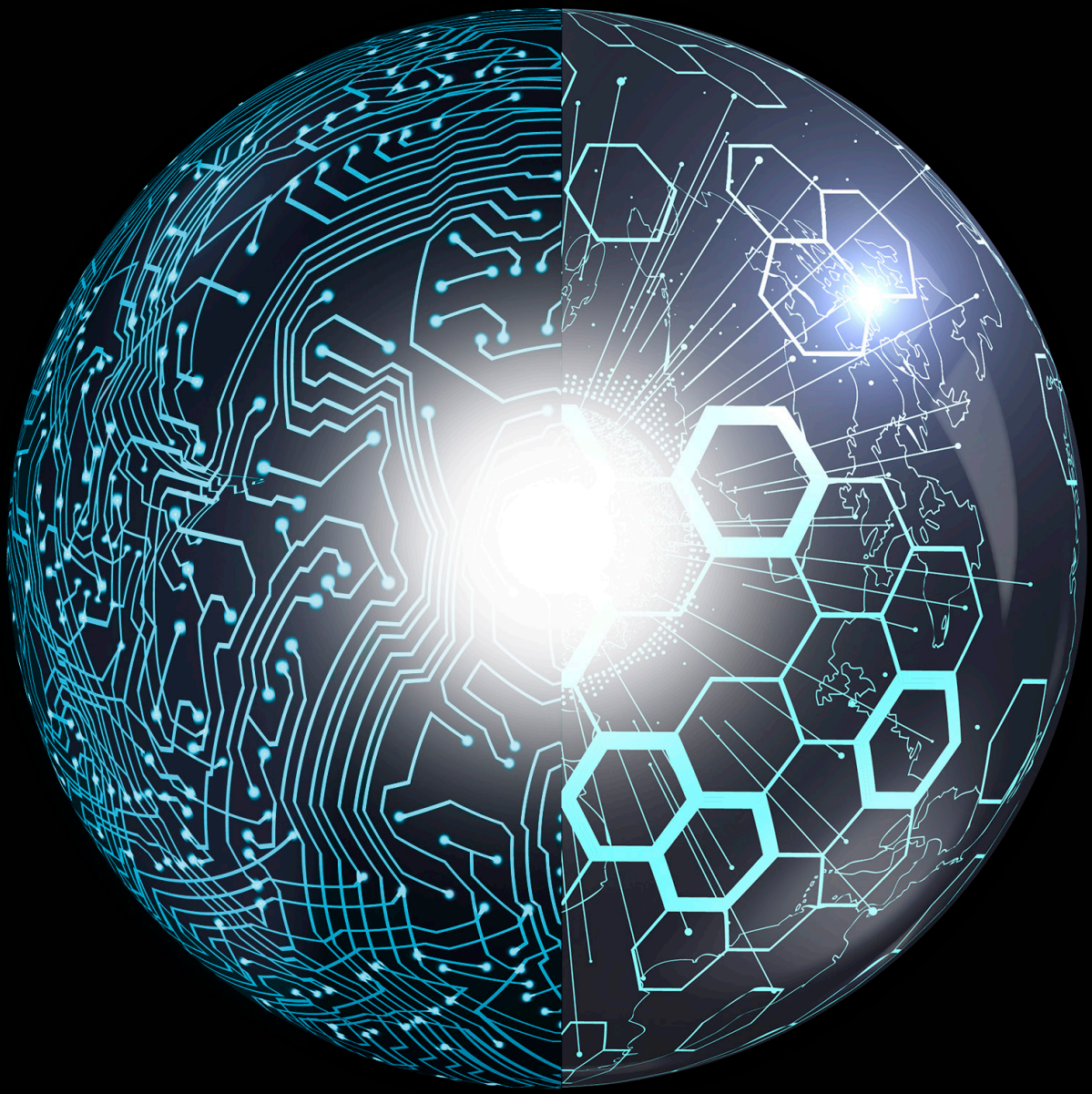
Deloitte.



Guarding the lifeblood of life sciences

Managing the risk of intellectual property cyber theft

Reframing the dialogue: What's a cyberattack?

The word "cyberattack" is typically associated with the theft of credit card numbers, health information, or other personally identifiable information (PII). Over the years, these types of breaches—and the regulations that help control them—have heavily influenced cybersecurity spending in many industries.

But for life sciences companies, breaches aren't the chief concern. The quiet undercurrent of targeted attacks to steal intellectual property (IP)—the lifeblood of life sciences companies—is a far greater threat. One study indicates that IP can constitute up to 80 percent of a company's value.[1] Nothing is likely to be more critical to a pharmaceutical company than the formula for one of its drugs. Or to a medical device manufacturer than the blueprint for its latest product.

Awareness of IP cyber risk may be rising.[2] But in the life sciences industry, IT security programs often relegate protecting IP from cyber theft to the back seat.

Relative lack of media coverage may be a factor, as companies typically aren't required to disclose incidents of IP cyber theft. And few choose to do so, fearing irreparable damage to their competitive advantage, market valuation, and brand. But given the extraordinarily high costs to bring products from development to launch,[3] a reexamination of priorities may be crucial in protecting company value.

.

Weighing the cost of protection against the cost of IP loss

How important is the investment to protect IP? For companies in certain industries—retailers facing credit card theft or banks facing cyber fraud—being the target of a cyberattack is extremely painful. But business models can be adjusted—perhaps through contingency funds or cyber insurance—to absorb occasional losses. Some cyberattacks, in other words, are viewed as a cost of doing business.

Theft of IP is an entirely different category of cyber risk—one that could threaten the very viability of a life sciences company. In a single instant, critical IP could be firmly in the grip of a competitor or rogue government, with the company none the wiser. Until it's too late. A competitor can potentially use IP theft to bring a strategic product to market faster than the company that invented it, or introduce fraudulent products that undercut profit margins or lead to extended litigation. Simply by no longer being solely in the company's hands, the IP has lost value, leading to potentially unrecoverable losses.

To dig deeper into the question of what's at stake, Deloitte used business valuation and financial loss calculation methods to simulate the business impact of a case of IP cyber theft against a technology company.[4] The exercise showed that for the fictitious victim, the overall financial impact exceeded $3 billion. This included not only the value of the IP itself but also a wide range of other factors, such as:

- Legal costs for investigation, litigation, and settlements, including potential class action suits
- Costs associated with executing a modified product strategy
- Impact to product revenue and margin if competitive products are introduced to market
- Loss of contracts or critical business relationships if theft of IP violates contract terms or impacts the interests of third parties
- Impact to reputation and company valuation if the incident is publicly disclosed

Though referencing a different industry, this example underscores the fact that commonly cited figures about the per-record cost of health information or other PII breaches have limited applicability in cases of IP theft. With a more realistic picture of the possible breadth and depth of impact, life sciences executives might determine that effective protection of their IP warrants greater investment.

IP thieves balance risks and rewards

Why is there growing concern in life sciences about IP theft? It's not only because cyber threats are more sophisticated and widespread than they used to be. Attackers, like good business leaders, focus on areas where returns are greatest relative to effort invested and where the likelihood of success is high relative to the risks of failure. From this perspective, life sciences IP may be an especially attractive target for attackers.

On the reward side, with a drug formula or product blueprint in hand—particularly pre-patent—thieves can substantially shorten delivery time and do an end run around massive development costs or reduce the effort to get a drug through regulatory hurdles. In areas where market opportunities are shrinking—as in the pharmaceutical sector, where there are fewer opportunities for a blockbuster drug to make its mark—the reward for stealing IP that targets a new area may be especially high.

Furthermore, the odds of a successful attack against a life sciences company may be higher than in other industries. Many organizations haven't invested in cyber risk programs in tandem with their evolving innovation and research and development (R&D) models. The pressures on life sciences companies to innovate faster and improve return on investment have increased dependence on digital information, network-based information-sharing, new connected relationships with consumers, and new forms of collaboration with third parties (such as external research organizations). These trends have widened the risk aperture. (See sidebar.)

Where cyber-related regulations haven't forced strong cybersecurity investments, a life sciences company's defenses and ability to detect and respond to attacks can be very weak, especially relative to the value of the IP it's holding. With an IP-focused cyber risk program, organizations can up the ante for the attackers and significantly alter the odds of becoming a victim.

A widening field of cyber risk
Prevailing trends in the life sciences industry that increase IP vulnerability include:

- **"Open innovation" and collaborative arrangements**: As more life sciences companies determine that a go-it-alone approach to R&D isn't viable, the data-sharing ecosystem has become increasingly complex. Every new joint venture, partnering arrangement, or contractor engagement enlarges the number of players with access to IP and other sensitive information.
- **Supply chain complexity**: The growing complexity of sourcing and supply chain models often requires the involvement of third parties with varying degrees of systems access. Poor security practices anywhere along the chain—from a supplier of raw materials to a logistics provider—can provide an open door for hackers to go after their ultimate objective.
- **Big data**: As R&D is fueled by enormous quantities of information from clinical trials, medical and other "smart" devices, and epidemiological studies, the centralization of this data—whether housed internally or in the cloud—makes it an attractive target.
- **Mergers and acquisitions (M&A)**: Vulnerabilities can be introduced as IT systems are integrated, especially if a target company doesn't have the same level of security as the acquirer—a factor often overlooked in the scramble to get a deal done. If an acquired company has already been breached—and it can be difficult to tell—hackers can gain access to the acquirer's data.
- **Digitization**: The digitization of R&D data, design records, formulas, and other IP-related artifacts makes them possible targets for theft regardless of a criminal's location.

Shifting the equation

Buying the latest security tool is a knee-jerk reaction for some organizations. But it's driven by fear, not by thoughtful strategy. No technology alone can protect against the intelligence, access operations, and capabilities of a sophisticated and ongoing cyber threat.

Deloitte encourages companies to take a *Secure.Vigilant.Resilient.*™ approach to managing cyber risk. The premise is that no environment is completely secure. Therefore, striving for perfect security likely isn't practical or cost-effective. Effective programs accept that some attacks will be successful and, rather than focusing only on keeping threats out, they balance four dimensions:

- **Secure**: Protecting critical assets against known and emerging threats
- **Vigilant**: Maintaining threat awareness and the ability to detect adversarial activity
- **Resilient**: Being prepared to recover quickly when incidents occur
- **Strategy and governance**: Making sure the three dimensions of the program (Secure, Vigilant, Resilient) are successful via oversight and metrics

Depending on the specific threats a company faces, which can shift over time as threats and business risk profiles change, some of these areas may be more important than others. Emphasis may also vary across areas of the business. Efforts to reduce the risk of IP cyber theft will look somewhat different from one company to another, but there are some important areas to consider that may apply to any life sciences company.

Secure

Within the realm of IT security, protecting sensitive data is paramount to a life sciences company. As a result, it's likely to be a core area for investment.

To optimally protect its IP, a life sciences company must first determine what it is and where it resides. From there, a robust classification system can inform the company's policies about how data should be handled and transferred, including who should have access to what information. As obvious as this seems, many organizations still have much to do to instill the discipline to establish this inventory and keep it up to date.

But countless attacks on corporate networks are launched when users, either maliciously or through ignorance or negligence, allow a hacker into their system. Educating the entire organization about phishing and other attack techniques can go a long way toward prevention.

Once inside the corporate environment, a hacker can more readily locate and tap into IP if users have access to data beyond what they actually need. Strong data protection goes hand in hand with strong digital identity management. It should also include mechanisms to prevent or limit potential damage by "privileged users," the trusted few who are granted high levels of data and system access to perform their functions.

Key questions

- How can we segregate our network, assets, and user access to optimize IP protection?
- What data requires the greatest access controls?
- Can we decentralize or distribute storage of sensitive information to make it more difficult for thieves to piece together valuable product designs or formulas?
- What data requires encryption?
- Have we established proper control mechanisms with the external parties with whom we share data?

Vigilant

Some top strategies to be vigilant against IP theft stem from two key characteristics of typical IP theft incidents:

01. IP theft is often targeted in nature. While instances of common data theft are frequently purely opportunistic, attempts to steal IP likely focus on a particular company for a specific reason. Because targeted attacks are usually executed in a series of steps over time, the actual presence of the enemy in the midst doesn't necessarily mean that IP has already been stolen. There are opportunities to detect and react to signs of infiltration along the way—provided there are good detection systems in place—to take action before actual data exfiltration occurs or to uncover and shut down an attack to limit the amount of data stolen.

02. IP theft is often perpetrated or heavily assisted by "insiders." Out of 29 cases of IP theft executed by foreign beneficiaries, the CERT Insider Threat Center found that 100 percent involved malicious insiders who "misused a company's systems, data, or network to steal IP."[5] Life sciences companies need to pay particular attention to the individuals who are accessing their IP, from employees to joint venture partners and other third parties. Working in tandem with talent departments, security teams can configure monitoring to look for warning signs of people who may be inclined to commit acts of theft.

The ability to detect signs of IP cyber theft isn't trivial. Effective programs require collaboration with talent leaders, line of business leaders, and other internal functions, tuning the granular design and execution of alerting systems to each particular business and technology environment.

Key questions

- Do we have the means to stay abreast of the tactics used by adversaries?
- Do we have the tools and capabilities needed to detect illicit attempts to gain access to IP?
- Do we have effective escalation procedures when signs of infiltration are detected?

Resilient

Once an incident has been discovered—preferably early in the course of an attack—rapid action is essential to shut down any leakage of information in progress and to make sure perpetrators are completely removed from all infected systems. Care should be taken to preserve forensic evidence that may be used during legal action or to support cyber insurance claims.

The response process is as much a business effort as a technical one. When theft occurs, a company must quickly assess the extent of the damage by determining what exactly was extracted. For example, was it an entire formula that was stolen or just a portion? What is the perpetrator likely to do with the information? There may be an opportunity to step up go-to-market activity or alter plans in order to reduce the impact of information exposure.

A strategy for resilience, though, starts before the need for resilience ever arises. Given that few organizations have fully equipped incident response skills in house, it may be wise to have pre-established terms with an outside firm that can fill expertise gaps. Having and rehearsing incident response plans—both the technical and business aspects of crisis response—are preparedness steps that can help reduce overall business impact

Key questions

- Do we have the analytic skills needed to quickly determine the impact of an infiltration?
- Are key leaders prepared to play the necessary roles when an incident happens?
- Do we have the ability to gather forensic evidence?
- Can our people respond effectively to limit the scope of an attack?
- Do our insurance policies cover cyber theft and offer sufficient coverage in the event of a breach?

What constitutes IP?

An important first step in designing an effective data protection and governance strategy is to draw a complete picture of what constitutes IP. Beyond the obvious—a drug formula or product blueprint—there are other forms of life sciences IP that may need to be included in the program scope. For example:

- Drug counterfeiters may be interested in packaging designs for a new drug to allow them to time the launch of their fraudulent product with that of the real one.
- Clinical trial data can be of particular interest to a competitor, if it wants to know in advance the strengths, weaknesses, and possible failures of a particular drug in development in order to determine a competitive approach.
- Government pressure to lower pharmaceutical costs has made pricing data a key target to competitors. Nothing could shake up the market more than seeing the price differences for the same drug in different countries.
- Product schematics that describe how to build a proprietary medical device could cripple the sales of a company that builds the product at a lower price.

The time is now

Providing strategy and governance for the agile *Secure. Vigilant.Resilient.* program

The possibility of cyber IP theft is such a sensitive business risk for life sciences companies that it calls for executive involvement and direction. Leadership is responsible for setting risk appetite, holding individuals accountable for the design and implementation of its IP protection program, and ensuring that cyber efforts receive the support they need—in terms of funding as well as the engagement of the right people.

Collaboration and mutual understanding between business and technology leaders is a cornerstone. Existing IP management processes should be reviewed to ensure that cyber risk issues are given the proper attention throughout the IP life cycle. To design and manage effective controls and monitoring, technologists must understand how IP is created and handled during normal business operations. R&D and other business leaders must understand when the decisions they're making have important ramifications for the cyber program to ensure that *Secure.Vigilant. Resilient.* components can be adjusted as needed—*proactively*, before an IP theft incident occurs.

This is doubly true in this era of transformation and innovation in life sciences. Careful examination of new forms of IP that are being created, new paths that are being laid for thieves to gain access to IP, and new *Secure.Vigilant. Resilient.* measures that may be warranted are integral to virtually every major business initiative—whether it directly involves the implementation of new technology or not. When many of these initiatives involve new forms of engagement with suppliers, research partners, or distributors, special attention must be paid to the cyber practices of those third parties.

Key questions

- Has the IP management program been updated to incorporate cyber risk issues?
- Are marketing, finance, R&D, and other leaders able to recognize potential cyber risk issues?
- Do technology leaders understand how IP should be handled?
- Do IT security and business leaders meet regularly and engage each other proactively?
- Are we properly considering IP cyber theft risks as we advance our innovation efforts?

Cyber incidents aimed at appropriating IP have the potential to cripple life sciences companies far more than the damage done by traditional data breaches. Loss of IP can not only harm a company's competitive standing and market valuation, but it can also cause rippling operational injury as the organization scrambles to adjust its business strategies to compensate. For this reason, it's imperative for life sciences companies to invest aggressively in protecting their IP beyond the minimum standards to meet compliance mandates.

While a *Secure.Vigilant.Resilient.* program is broad and involves many aspects of an organization, building and improving such a program is an evolutionary process. Many companies have a lot of catching up to do. But regardless of their current maturity level, most organizations have a solid starting point in each of the three areas that, with strong executive sponsorship, can be used as a foundation for incremental, phased improvements.

The time to commit to these advances is now. The technology-enabled innovation and digital transformation efforts that are so essential to the future of life sciences companies justifiably consume significant resources. And unless proportionate attention is paid to protect the organization's lifeblood—its IP—a single instance of IP theft could undermine the benefits these innovations are expected to yield. Integral investments in proactive management of cyber risk are a critical success factor for tomorrow's industry leaders. A robust and proactive cyber risk management strategy is critical for tomorrow's leaders who are seeking to lead, navigate, and disrupt in the life sciences industry.

Contact us

Larry Samano
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
lsamano@deloitte.com

Keith Brogan
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
kbrogan@deloitte.com

Jason Frame
Specialist Leader | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
jframe@deloitte.com

Endnotes

1. News Release: Annual Study of Intangible Asset Market Value from Ocean Tomo, March 5, 2015, Ocean Tomo, LLC, http://www.oceantomo.com/2015/03/04/2015-intangible-asset-market-value-study/.
2. The 2015 Deloitte Regional Cybersecurity Survey showed that 44 percent of executives named protection of IP or strategic proprietary information as one of their top cyber risk concerns. Source: https://www2.deloitte.com/ca/en/pages/risk/articles/cybersecurity-survey-2015.html.
3. For pharmaceutical companies, for example, the average cost to bring a compound from discovery to launch hovers at about $1.5B. Source: "Balancing the R&D equation: Measuring the return from pharmaceutical innovation 2016," Deloitte LLP, 2016, https://www2.deloitte.com/uk/en/pages/life-sciences-and-healthcare/articles/measuring-return-from-pharmaceutical-innovation.html.
4. John Gelinne, J. Donald Fancher, and Emily Mossburg, "The hidden costs of an IP breach: Cyber theft and the loss of intellectual property," Deloitte Review, Issue 19, Deloitte University Press, July 2016, https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html.
5. Matthew L. Collins, Derrick Spooner, et al., "Spotlight On: Insider Theft of Intellectual Property Inside the United States Involving Foreign Governments or Organizations," Carnegie Mellon University Software Engineering Institute, May 2013, http://www.sei.cmu.edu/reports/13tn009.pdf.

Deloitte.