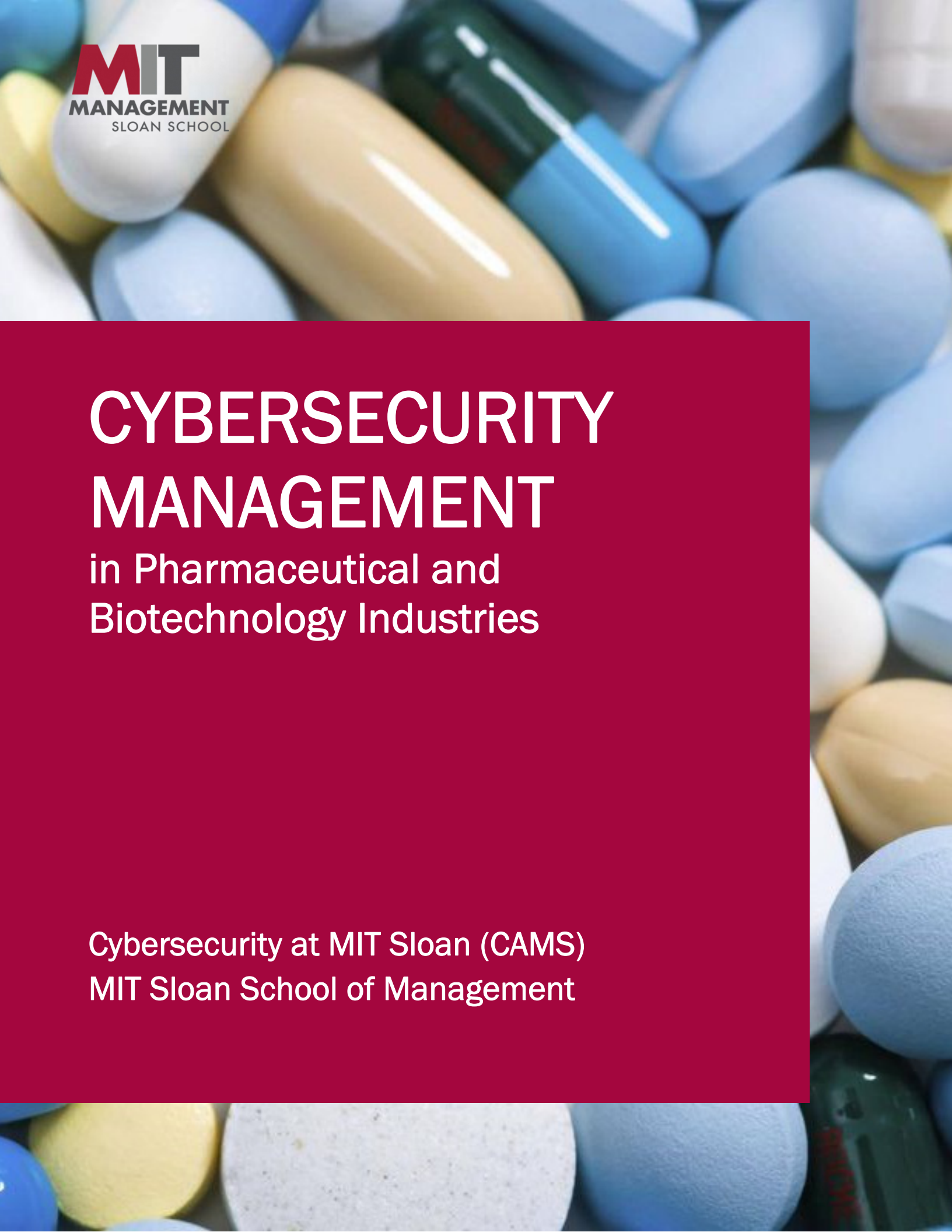


MIT MANAGEMENT SLOAN SCHOOL

CYBERSECURITY MANAGEMENT

in Pharmaceutical and Biotechnology Industries

Cybersecurity at MIT Sloan (CAMS)
MIT Sloan School of Management

In 2015, cybercrime damages cost the world an estimated $3 trillion. Cybersecurity Ventures predicts that by 2021, that number will increase to an annual $6 trillion.

Pharmaceutical and biotechnology companies face industry-specific issues that make cyber defense critical but also more challenging. Even a company that understands the need for cybersecurity will have difficulty conceptualizing what is at stake, and staying up to date with the changing cyber threat landscape.

Cybersecurity at MIT Sloan provides research about the latest cybersecurity risks and threats, as well as innovations and methods to fight back against cyber attackers.

Pharmaceutical and Biotechnology Industries

An Attractive Target

Today, the pharmaceutical and biotechnology industries face significant cybersecurity challenges. These industries offer an attractive target for cyberattacks because of their substantial investment in research and development, valuable intellectual property, connected IT and operational networks, and sensitive stores of data. According to the Cisco 2014 Annual Security Report, the Pharmaceutical Sector was a much greater target than other sectors. In fact, the amount of malware targeting Pharmaceuticals was just over 600% of the median across all industries. Though more recent industry-specific data is not available, Cisco reported an increase in the scale and sophistication of malware as of 2018.

High Costs

Malware encounters can immensely impact pharmaceutics and biotechnology organizations. The 2017 NotPetya cyberattack on Merck & Co.—which affected its global manufacturing, research, and sales—cost the company over 300 million USD, just in one quarter. An outside hacker can access or manipulate data and production processes, and an insider threat poses even greater dangers, like theft of trade secrets or corporate cyber-espionage.

Consequences of a cyberattack can include stolen IP, repeated clinical trials, litigation, a frightening amount of lost revenue, and most importantly, damage to a company's reputation. Victims of theft not only face massive internal issues but also find themselves targeted by class action lawsuits and regulatory actions. Technological solutions have proven insufficient in protecting organizations, and the importance of comprehensive cybersecurity management in pharmaceutics and biotechnology is greater than ever.

Cybersecurity Challenges

The pharmaceutical and biotechnology industries face the following major cybersecurity issues:

TECHNOLOGICAL CYBERSECURITY ISSUES

Intellectual Property

A new drug formula is one of the most valuable assets a pharmaceutical or biotechnology company can possess. Theft of this kind of IP exposes a company to litigation risks, as well as insurance implications. Lack of good safeguarding can make a firm's trade secrets accessible through processes like spear phishing or zero-day exploits.

Vulnerable New Technologies

As pharmaceutical and biotechnology companies adopt innovative new tools such as cloud computing and big data analytics, they also increase their risk of cybersecurity issues like data leakage. Because of the proliferation of devices that collect and distribute health data, cybercriminals can more easily exploit this critical data. Furthermore, new privacy regulations bring data protection concerns into public focus.

Mergers and Acquisitions

Pharmaceutical companies are inadvertently putting themselves at risk through mergers and acquisitions that involve the aggregation or division of technological infrastructure and company property. A company may face serious liabilities if it cannot protect confidential data. Without proper protection measures, a merger or acquisition presents an opportunity for hackers to steal and sell information on the dark net.

Industrial Control Systems

The increased connectivity of computers and manufacturing systems means that hackers can target physical production processes. Due to the failure of Merck and Co.'s network during the 2017 attack, the company was forced to halt production of its drugs across the board, with some of its processes taking months to resume. The automation and network connectivity of industrial control systems requires strong security and oversight.

Employees know hackers are gunning for them, yet they keep falling for hackers' tricks. Companies can change that.

HUMAN CYBERSECURITY ISSUES

Untrained Staff

Employees unfamiliar with cyberattack contingency plans or the threats of hacking can put an entire company at risk. An employee who has not received *effective* training in cybersecurity might input credentials in a fake login page, or accidentally download malware with a careless click. For instance, our research found that even after extensive training, 5-10% of employees in healthcare organizations still clicked on phishing links.

Insider Threat

Employees recognize the value in IP and other confidential information. Insiders can therefore gain personal advantage from the unauthorized misuse of IP. The current cybersecurity reports show that the healthcare industry suffers most from insider threats.

Governance

Cybersecurity is often overlooked at the executive level, or relegated to an "IT issue" which top management ignores. To protect themselves from the risks outlined above, pharmaceutical and biotechnology companies must develop a strong security program with contracts, an operating model, delegated roles and duties, and a consistent form of communication. Often, companies lack top-level prioritization required to install complex, company-wide, effective data protection.

Third Parties

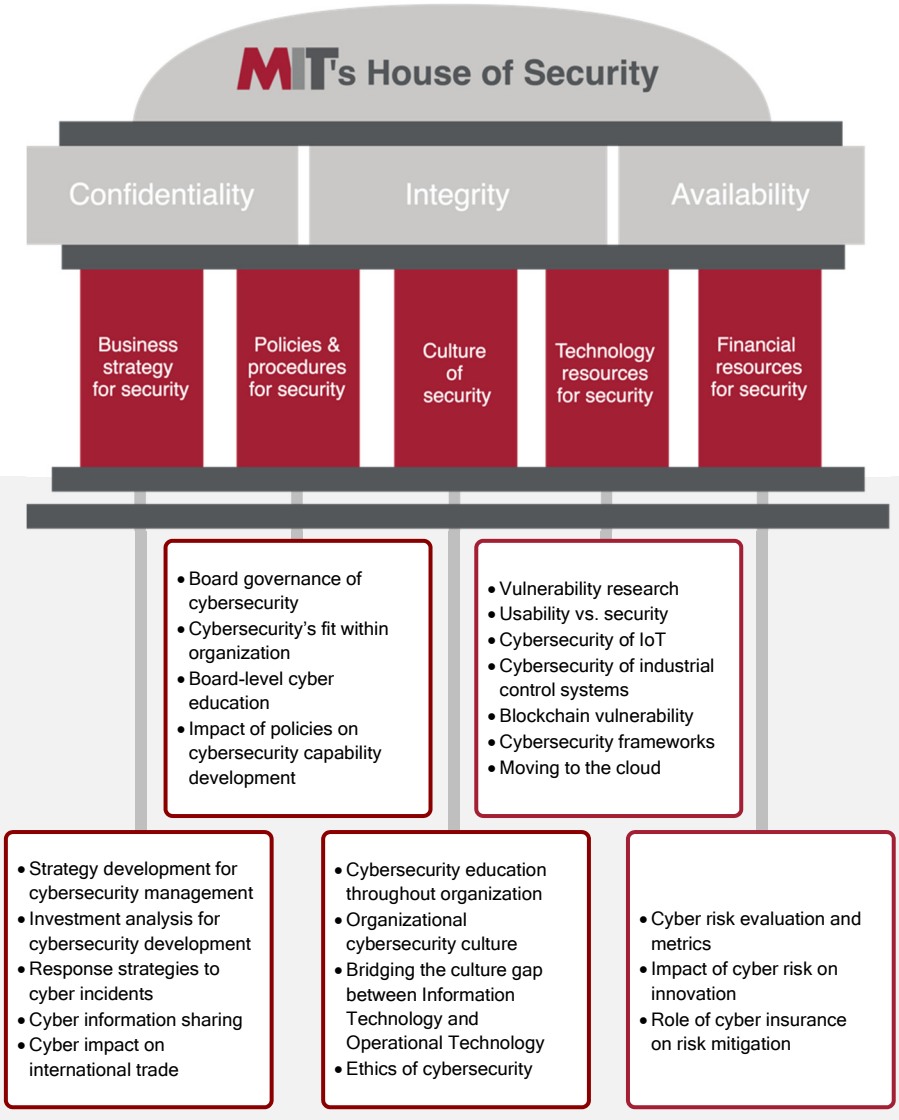
Third-party relationships are critical to the sales and operations of pharmaceutical and biotechnology companies, but they also introduce greater complexity to cybersecurity management. With so many suppliers, suppliers of suppliers, and vast information handling, it becomes extremely difficult to implement consistent security protocols for all parties with access to company data.

Cybersecurity at MIT Sloan (CAMS)

Cybersecurity at MIT Sloan (CAMS) brings together thought leaders from industry, academia, and government with MIT faculty, researchers, and students. The group studies the strategy, management, governance, and organization of cybersecurity using an interdisciplinary approach. CAMS provides a confidential academic forum in which leaders and managers can benefit from the experiences of CSO/CISOs across multiple sectors.

Researchers and faculty work directly with companies to conduct projects that address the unique, unresolved issues surrounding a range of industries, working to establish material solutions that will shape the future of cybersecurity. MIT's house of security framework below presents the five major areas of research (cardinal color) conducted by CAMS, along with examples of projects for each area.

Expert faculty
Innovative ideas
Renowned research



Join us at the forefront of groundbreaking cybersecurity developments, and increase the return on your investments.

Website:
https://cams.mit.edu

CAMS research director for pharmaceutical and biotechnology industry:
Dr. Mohammad Jalali ('MJ'): jalali@mit.edu

CAMS directors:
Dr. Keri Pearlson, CAMS Executive Director: kerip@mit.edu | Dr. Stuart Madnick, CAMS Co-director: smadnick@mit.edu | Dr. Michael Siegel, CAMS Co-director: msiegel@mit.edu