Cybersecurity at MIT Sloan (CAMS)

Cybersecurity Management in Pharmaceutical and Biotechnology Industries

An Attractive Target

Pharmaceutical and biotechnology companies 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. 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.

Unique Challenges

+ Mergers and Acquisitions

Pharmaceutical and biotechnology companies are inadvertently putting themselves at risk through mergers and acquisitions that involve the aggregation or division of technological infrastructure and company property.

+ 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.

+ Industrial Control Systems

The increased connectivity of computers and manufacturing systems means that hackers can target physical production processes.

+ Human Errors

Employees unfamiliar with cyberattack contingency plans or the threats of hacking can put an entire company at risk; 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.

+ 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.

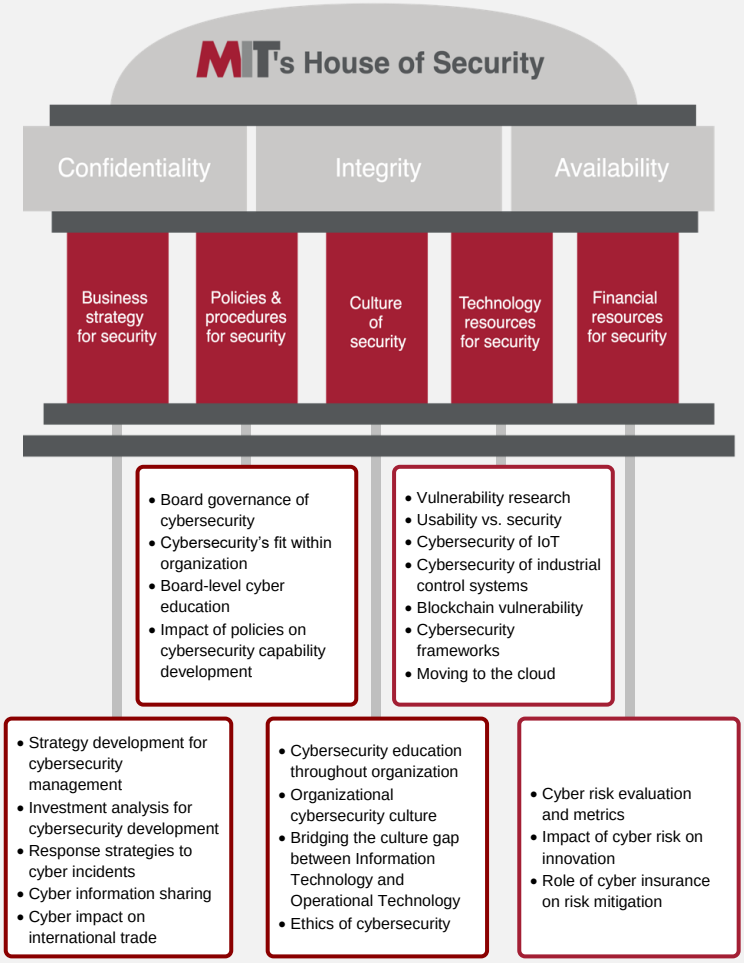
Research from CAMS Addresses These Challenges

Expert faculty. Innovative ideas. Renowned Research.

Cybersecurity at MIT Sloan (CAMS) brings thought leaders from industry, academia, and government together with MIT faculty, researchers, and students. Our goal is to answer the most difficult questions about the strategy, governance, management and organization of cybersecurity using an interdisciplinary approach. CAMS provides a confidential academic forum in which members benefit from the experiences of CSO/CISOs across multiple sectors.

MIT's House of Security framework presents the five major research areas (cardinal color) addressed by CAMS, along with examples of projects for each area.

Join CAMS for access to the latest research and innovative solutions for managing and leading cybersecurity.



Website:
https://cyber.mit.edu

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

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