Kiteworks

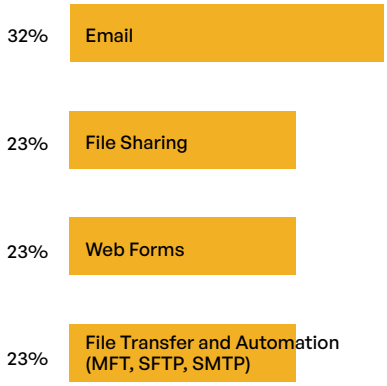
Sensitive Content Communications Privacy and Compliance in Manufacturing

Highlights from Kiteworks' "2022 Sensitive Content Communications Privacy and Compliance" report

MANUFACTURING BRIEF

Intellectual property (IP)—which includes R&D, engineering, and operations data—is a key target for nation-states and malicious cybercriminals for manufacturers. Over one-third of manufacturing executives say IP theft is the primary motive behind cyberattacks on their companies.[1] The risk of confidential data breaches in manufacturing is heightened by supply chain interdependencies, two-way data streams, embedded but unmanaged endpoints, and adoption of cloud computing.

What Sensitive Content Communications Channel Poses the Greatest Risk?



Cyberattacks on manufacturers can take different forms—on data in transit and at rest. Social engineering attacks use phishing and spear phishing to impact systems or ransomware that holds company data hostage until the hacker's demands are met. Network, application, and endpoint vulnerabilities—both known and unknown—can be exploited to gain access to IP. Man-in-the-middle attacks target sensitive content communications that fails to employ encryption and other security protocols.

According to a new IBM report, manufacturing was the most attacked industry last year—overtaking financial services and insurance that ended a long run at the top of the industry list.[2] Nearly half of attacks on manufacturers targeted vulnerabilities that had not yet or could not be patched. The most prevalent attack types included ransomware (23%), server access (12%), and business email compromise (10%).[3]

Security and Compliance Governance

Manufacturers share critical information internally between different departments as well as across their distributed supply chains using various communication channels. Following are some of the more prevalent use cases:

- Protecting IP related to designs, plans, financial documents, marketing content, and contracts
- Complying with privacy regulations that govern personally identifiable information (PII) in invoices and other documents

- Adhering to Cybersecurity Maturity Model Certification (CMMC) standards for the exchange of controlled unclassified information (CUI)
- Complying with GxP by ensuring secure and immutable transfers of manufacturing quality data across Purdue Model levels
- Automating secure exchange of orders, schedules, invoices, designs, and other information with supply chain partners
- Securing exchange of large, terabyte-sized CAD and other large files with internal plants and departments and various third parties in the supply chain

All the above are governed by various compliance standards that start with data-related PII, protected health information (PHI), security foreign corruption and bribery, and securities. Privacy regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), Personal Information Protection and Electronic Documents Act (PIPEDA), and California Consumer Privacy Act (CCPA), govern PHI and PII, whereas other regulations are more industry specific. And as artificial intelligence, which often relies on big data, becomes increasingly more important in manufacturing, tracking and controlling that data grows accordingly—specifically how sensitive manufacturing data is shared and stored.

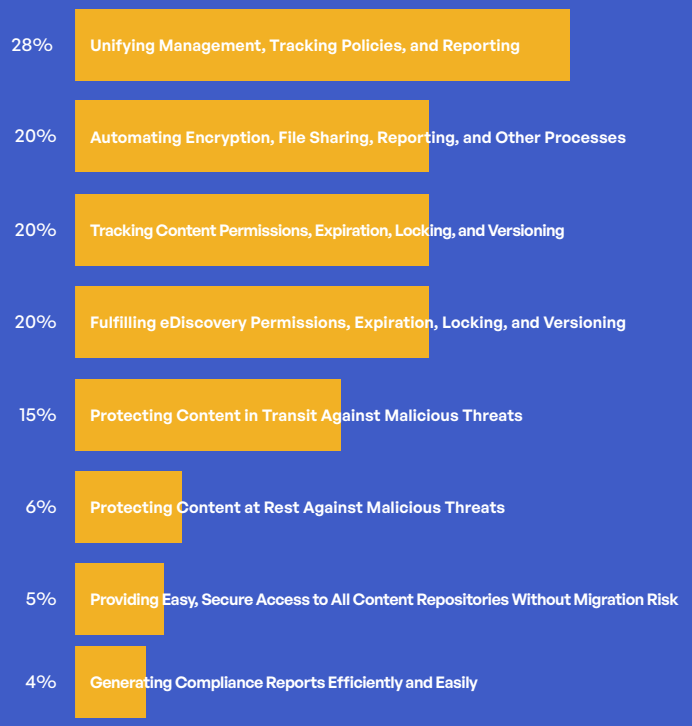
Private PHI Communications With Third Parties

In addition to all data that is shared internally, manufacturers exchange a lot of sensitive data with third parties. Depending on the regulation or standard, policies are specified around data type, user and device access, data classification, cataloguing, and expiration, and audit trail reporting. Manufacturers must have the right governance tracking and controls in place for privacy and compliance of data that is at rest and in motion. Challenges around the supply chain post-pandemic and threats targeting manufacturers lacking encryption and governance controls can be exposed to malicious third-party actors.

One of the biggest challenges involves the sharing and transfer of data with third parties. The following graphic examines some of the manufacturing findings.

What Are Your Top Concerns in Managing Sensitive Content Communications?

What Are Your Top Priorities Around Third-party Sensitive Content Communications?



Governance, Risk, and Compliance Survey Findings

Based on findings from a survey conducted by Kiteworks and Survey Pacific in early 2022, 34% of manufacturers indicate their organizational governance and protection of sensitive content communications either requires a new approach or needs significant improvement (another 38% indicate some improvement is needed).[4] A likely reason is the lack of technologies and processes to measure risk: fewer than half (47%) have technologies and processes in place to do so.

Only half (50.5%) of respondents believe their organizations are well-protected when it comes to third-party risk. Communications in the cloud is a problem for many manufacturers: 48% either do not manage and monitor sensitive content shares and transfers in the cloud or only manage and monitor some of them. More than half (52%) of manufacturers say they must generate over seven compliance reports annually. However, despite all the time and resources spent on compliance, 19% of respondents indicate their compliance reports are only somewhat accurate (another 62% say they are mostly accurate).

Governance

69%

use 4 or more systems for tracking, controlling, and securing sensitive data communications with third parties

23%

believe their governance and protection of third-party content communications either requires a new approach or requires significant improvement (another 38% say some improvement is needed)

47%

have technologies and processes in place to measure risk associated with third-party content communications (the remaining 53% plan to do so)

Risk Management

38%

use antivirus and antispam technologies to verify all incoming data communications from third parties

48%

use DLP for file sharing and file transfer with third parties

52%

encrypt less than 75% of their content communications with third parties

39%

indicate their risk management and security of third-party content communications requires a new approach or significant improvement

49%

believe their organization is not well-protected against third-party content communication risks

48%

either do not or only manage and monitor some content communications in the cloud

Compliance

52%

must generate over 7 compliance reports annually

36.5%

spend over 40 hours generating each compliance report (15% spend 80-plus hours)

19%

feel their compliance reports are fully accurate, with 59% saying they are mostly accurate (not contain errors)

Kiteworks Private Content Network Provides Governance, Compliance, and Security

Kiteworks enables manufacturers to create a dedicated Private Content Network (PCN) of internal and external digital communications that ensures privacy and compliance of sensitive content—ranging from PHI and PII information to proprietary IP-related content. The supply chain has become a critical focus as global economies emerge from the COVID-19 pandemic, and this is the key reason manufacturing is now the number one industry vector when it comes to cyberattacks. When data breaches do occur, the cost can be dramatic. While the average cost of a data breach in manufacturing declined year over year, it is high at $4.24 million (the average across industries).[5]

Kiteworks enables manufacturers to protect critical IP related to product design, prototypes, production schedules, and supply chain logistics. Manufacturers also share and store PII for their employees, customers, and partners, which can be hacked in transit and in motion. Unifying, tracking, controlling, and securing this sensitive content with the Kiteworks platform creates a Private Content Network (PCN) for manufacturers that is fully secure and compliant with various standards and regulations.

For these and other highlights from Kiteworks' "2022 Sensitive Content Communications Privacy and Compliance" report, download a copy.

References

[1] "Cyber risk in advanced manufacturing," Deloitte and MAPI, accessed March 31, 2022.

[2] "X-Force Threat Intelligence Index 2022," IBM Security, February 2022.

[3] Ibid.

[4] "2022 Sensitive Content Communications Privacy and Compliance Report," Kiteworks, April 13, 2022.

[5] "Cost of a Data Breach Report 2021," IBM and Ponemon Institute, July 2021.

Kiteworks