Crowe

Checklist

Six questions M&D companies should ask about cybersecurity

Audit / Tax / Advisory / Risk / Performance

Smart decisions. Lasting value.™

Cybersecurity attacks continue to cost businesses millions of dollars annually. Although high-profile attacks in the government, retail, and financial sectors often generate headlines, manufacturing and distribution (M&D) businesses are equally vulnerable to unauthorized intrusions that compromise sensitive data. Here are six critical questions M&D technology and information security officers should be asking about their cybersecurity systems.

Cybersecurity failures are becoming increasingly common in a world where billions of devices, systems, and data stores are now interconnected. The resulting damage is often widely publicized, difficult to repair, and extremely expensive. In some cases, cyberattacks have such a profound impact on a company's systems that it is difficult even to assess the full extent of the damage.

High-profile attacks in government agencies and in the financial services, retail, and entertainment industries usually garner the most media attention, but companies in the M&D sector are just as vulnerable to the loss, theft, or destruction of sensitive data. So it is incumbent on M&D businesses to put in place the same cybersecurity essentials that other vulnerable businesses implement including:

- A formal and thorough cybersecurity program
- Clearly defined responsibility for cybersecurity issues including a designated cybersecurity officer
- Well-defined, up-to-date procedures for detecting and containing attacks
- Detailed, regularly updated incident response plans

Beyond these core elements, M&D companies often face challenges that are specific to their industry. The following list is designed to assist technology and information security officers with identifying their organization's own particular vulnerabilities. These are questions they should be asking themselves about their company's current cybersecurity capabilities, gaps, and requirements.

Where does our data actually reside?

Do we have an up-to-date inventory of all databases, file sharing, and storage systems? What standards are in place for protecting data in these facilities? Are these standards regularly updated? How is compliance monitored?

The first step in protecting data is to identify the types of information you have and where that data resides, including databases, file sharing systems, local devices, and individual applications. Crowe cybersecurity risk specialists can help with data mapping, risk assessments, and records management inventories.

Crowe also has extensive experience helping companies develop standards and controls to minimize the transfer of critical data to unauthorized storage devices.

How do we control access to sensitive data and accounts?

Who has the "keys to the kingdom"? Do we regularly monitor the activities of those with access to sensitive data? Do we regularly review our account management controls to reflect current needs and assignments? Do we maintain accountability for shared accounts on the floor? How do we handle the departures of personnel with sensitive access?

An effective cybersecurity program requires more than just technology solutions – it must focus as well on the people and policy issues that are critical to security. For example, many M&D organizations still manage multiple critical production processes and systems through shared accounts, creating an inherent lack of accountability. Another common weakness involves administrator accounts that have no effective third-party review or access if a key administrator leaves.

Crowe data protection specialists can map how your organization handles, processes, and stores data. They can then offer detailed recommendations for more effective policies and procedures to improve controls, set up alerts, design methods to prevent hacking, and implement appropriate backup, cross-training, and system audits.

✓ What steps do we take to log and monitor cybersecurity risk?

Have we tuned and customized our security information and event management (SIEM) system to look for attacks? Are we testing the SIEM for effectiveness? Have we integrated all layers of technology into the SIEM?

SIEM systems are widely used to aggregate and correlate the numerous event logs that are integral to various technology systems, including networks, databases, servers, and individual applications. To be effective, a company's SIEM system must be customized and tuned to integrate all layers of technology into the company's unique system environment.

Beyond merely aggregating the information, however, the SIEM system must also be configured to identify particularly sensitive data and to apply intelligent analysis in order to recognize specific event patterns that could indicate both basic and advanced types of attacks. Crowe cybersecurity teams have extensive experience in implementing, configuring, and testing SIEM technology.

✓ How do we manage cybersecurity risk from vendors and other third parties?

What data are we sharing with third parties? What systems are they allowed to access? What steps do we take to track or monitor vendors with sensitive access? Do we rank vendors by risk?

As M&D organizations outsource significant portions of their processes to third-party vendors and cloud providers, the risk of data breaches increases due to the outside parties' access to critical systems and information. Crowe third-party risk management services can help you evaluate vendor security – both at the time of selection and through periodic reviews – by assessing individual relationships and identifying discrepancies among their information security policies, your own processes, and industry-accepted best practices.

Whether performing detailed security or penetration assessments, inventorying and protecting organizational data, improving third-party security, or designing solutions to improve IT resilience, Crowe can provide pragmatic solutions to help your organization maintain a consistent security posture.

What are we doing to address wireless security concerns?

Which of our systems and processes have been shifted from wired to wireless systems? What tools are in place for guest network segmentation? How do we secure virtual local area networks (VLANs)?

With radio-frequency identification (RFID) scanners and other smart devices now commonplace in many M&D environments, a growing number of organizations are increasingly vulnerable to unauthorized access to their VLANs, where critical data production and financial data reside. Crowe information security teams can help you verify that unsecured guest networks are properly segmented from the corporate network and internal infrastructure.

In addition, Crowe teams are experienced in implementing systems that sufficiently encrypt data, authenticate valid endpoints, and deny unauthorized access to wireless networks.

How do we manage security for legacy systems that are no longer supported?

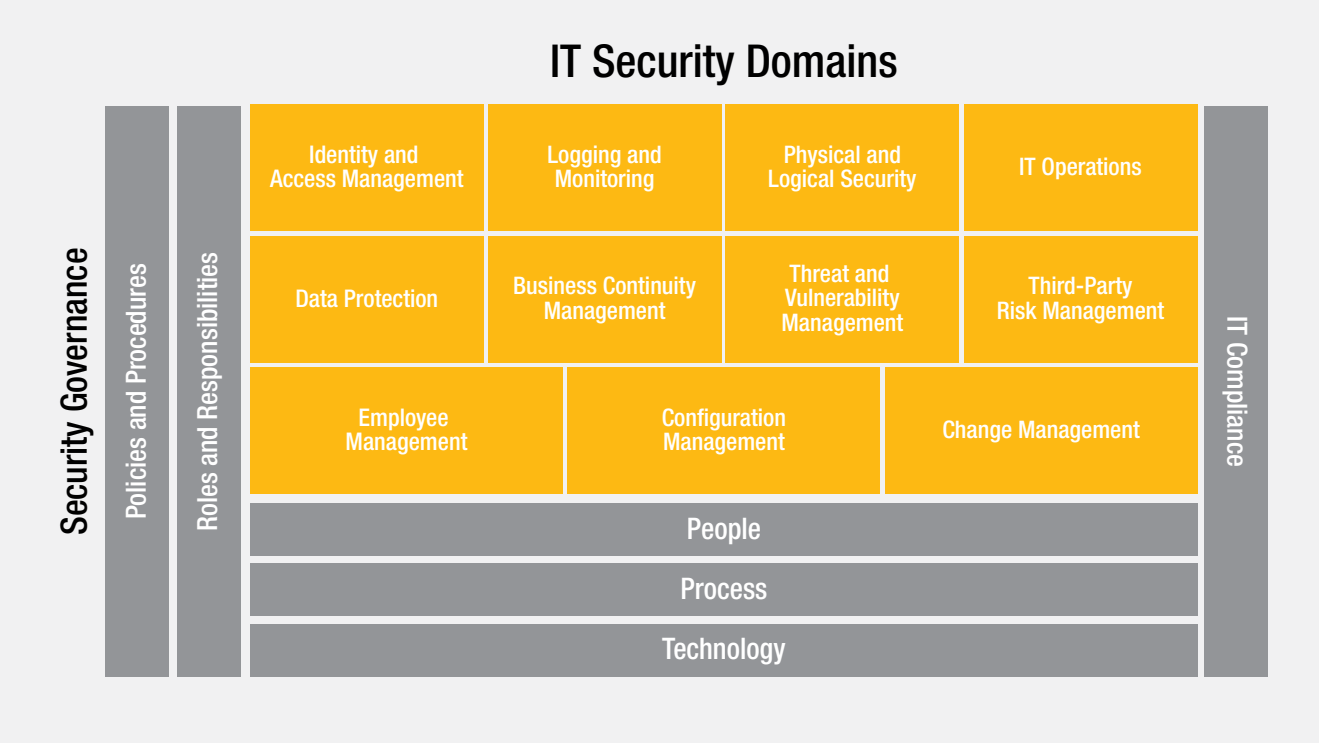
What legacy systems do we rely on that can no longer be patched or updated? What compensating controls are in place for these systems? How are these systems incorporated into our organizational risk management approach? What steps are we taking to replace these systems?

Modern M&D organizations typically rely on a variety of highly specialized or customized production software applications, which over time become outdated or are no longer supported by their original providers. Although running software past its support date is never recommended, a variety of business reasons might make it necessary. Often, viable replacement applications are either unavailable or prohibitively expensive – yet retaining outdated software is a risky tactic that introduces the possibility of new vulnerabilities that cannot be patched or updated.

Crowe information security teams can help identify such vulnerable legacy systems and help implement compensating controls that can aid in bringing the risk of these systems to an acceptable level.

Next steps – applying a framework for risk management

Crowe data-loss prevention services can help M&D organizations identify flaws in the tools and methods they use to protect sensitive information. By applying the Crowe cybersecurity risk framework (see Exhibit), Crowe specialists can help you recognize and address your organization's unique vulnerabilities and apply a rational, structured approach that is both practical and responsive to today's fast-changing threats.



Source: Crowe analysis

Learn more

For more information, or to schedule a more detailed discussion of your specific cybersecurity risks and concerns, contact Crowe or visit www.crowe.com/cybersecurity.

Christopher Wilkinson, Principal
+1 214 777 5288
christopher.wilkinson@crowe.com

crowe.com

Text created in and current as of October 2016; Cover and artwork updated in May 2018.

RISK-17005-020A