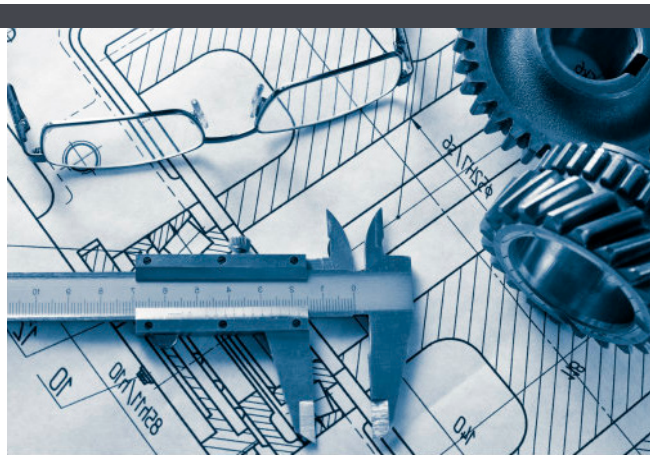
Manufacturing Cyber Security Guide



The Manufacturing Cyber Challenge

Our world has been radically transformed by digital technology – smart phones, tablets, and web-enabled devices have altered the way we manage production and do commerce. At the same time, technology has enabled a new generation of criminals to gain access to critical parts of a business's infrastructure. In the Manufacturing sector, economic security is directly linked to cybersecurity, and a halt to production can be crippling.

The National Association of Manufacturers estimate that $239.9 billion in revenue has been lost to cyber-related issues over the past ten years. And the trend is accelerating – it's far less expensive for a rival company or government to hire a hacker than compete with a business themselves. Verizon's 2016 Data Breach Investigations Report (DBIR) identified Manufacturing as one of the most victimized industries by hackers, with companies of all sizes equally targeted. Criminals are finding creative ways to infiltrate today's manufacturers, from factory floors to refineries, as they become more connected.

The Solution

The transition of business processes to the cloud and proliferation of connected endpoints increase the vulnerability of critical access to outside threats. IT managers must implement more comprehensive policies regarding the secure handling and transmission of data.

The four key components of a solid internet and data security program include:

- Advanced Threat Defense
- Education of Staff, Vendors and Associates
- Data Protection Services
- Endpoint Security

Advanced Threat Defense

Email is a primary threat vector by which hackers access your data. It's easier for a hacker to send out an email than to hack a firewall – it takes just one unsuspecting staff member to open the wrong email or click a bad link to punch a hole in your network defense. EdgeWave's ePrism Email Security Suite includes the powerful tools you need to assure the protection of private data and the efficient delivery of legitimate email. ePrism offers fully hosted in-the-cloud services that require minimal management, are affordable, and can scale easily to fit any size network.

ePrism includes a multi-layered approach that stops emerging threats before they can get near your network. EdgeWave cybersecurity solutions combines human threat review and automated intelligence to identify and stop advanced threats in real time. Humans can identify the intent of inbound threats in a way an algorithm can't – that's why every cyber security plan must include human analysis. In 2016 alone, EdgeWave's human review process has blocked over 120 million malicious emails per day with human-written rules and analysis. The 2016 Verizon Data Breach report promised "We may be able to reduce the majority of attacks by focusing on a handful of attack patterns." EdgeWave leads the market with this capability.

Data Protection Services

Data Loss Protection (DLP) - ePrism includes a content analysis and policy engine that uses proprietary technology to detect private information transmitted via outgoing email. This data protection technology analyzes data in motion, and using compliance-based rules, detects and blocks any sensitive private data trying to leave your network. This solution is easily managed from the ePrism Central Dashboard giving you the powerful tools you need to ensure the safety of your most valuable corporate assets.

Encryption - EdgeWave Email Encryption assures the secure delivery of email to anyone outside your network, with next-generation technology that eliminates the cost and complexity associated with many traditional encryption services. As a completely hosted service, there is no hardware or software to implement and encryption can be easily enabled on a per user basis or as part of an automated routing policy. In addition, because it is integrated into the ePrism Hosted Email Security and Data Loss Protection

services, your outgoing email is inspected for malware, viruses, inappropriate content, compliance breaches and violations of your acceptable use policy (AUP). You can manually encrypt messages or configure to automatically encrypt per a variety of factors; such as sender, recipient, or when DLP problems are detected.

Endpoint Security

Laptops, smartphones and tablets have improved productivity and efficiency by empowering managers to keep tabs on resources and processes at the swipe of a finger, while freeing up workers to exercise greater independence and mobility. But this also brings risks, with Ponemon Institute's Global Study on Mobility Risks reporting a majority (59 percent) of companies seeing employees "circumvent or disengage security features" in their company-sponsored mobile devices, while 51 percent have experienced data loss due to improperly secured mobile data.

iPrism Web Security can help you mitigate endpoint risk with Cloud-Based Remote Web Filtering and Mobile Device Security. These security solutions employ proprietary technology to bring powerful Enterprise Web Filtering to all staff and devices, even outside the network. You receive comprehensive protection from web-based threats, granular policy controls, and selective data wiping -- all with centralized administration and reporting. Suitable for both corporate and BYOD devices, iPrism provides anytime, anywhere any device security for iPads, iPhones, Android devices, Windows laptops and Macbooks.

Education of Staff, Vendors and Associates

The internet and data security technologies described above are only as effective as the training and policies that enforce their use. Here are 5 steps to get you started on the path to ensuring your organization will support your security efforts:

1. Integrate a security strategy with every plan and initiative. Isolate valuable assets and restrict who has access to them
2. Empower employees with targeted, plain-English security training. Manufacturing is largely self-regulated, and educated employees are your best line of defense
3. Implement and enforce strong organizational/IT policies regarding social media and portable devices.
4. Ensure all employees and vendors know how to guard authentication credentials. Require a signed and sealed agreement of understanding and adherence to privacy policies
5. Employ an agile, robust, platform-agnostic, advanced threat detection system that includes encryption

EdgeWave's award winning solutions have helped thousands of manufacturing organizations protect their data and networks. EdgeWave offers cloud-based services as well as on premise appliances for email and Web security services that require minimal management, are affordable, and can scale easily to fit any size network. To learn more about EdgeWave and its powerful solutions, please visit https://www.edgewave.com/.