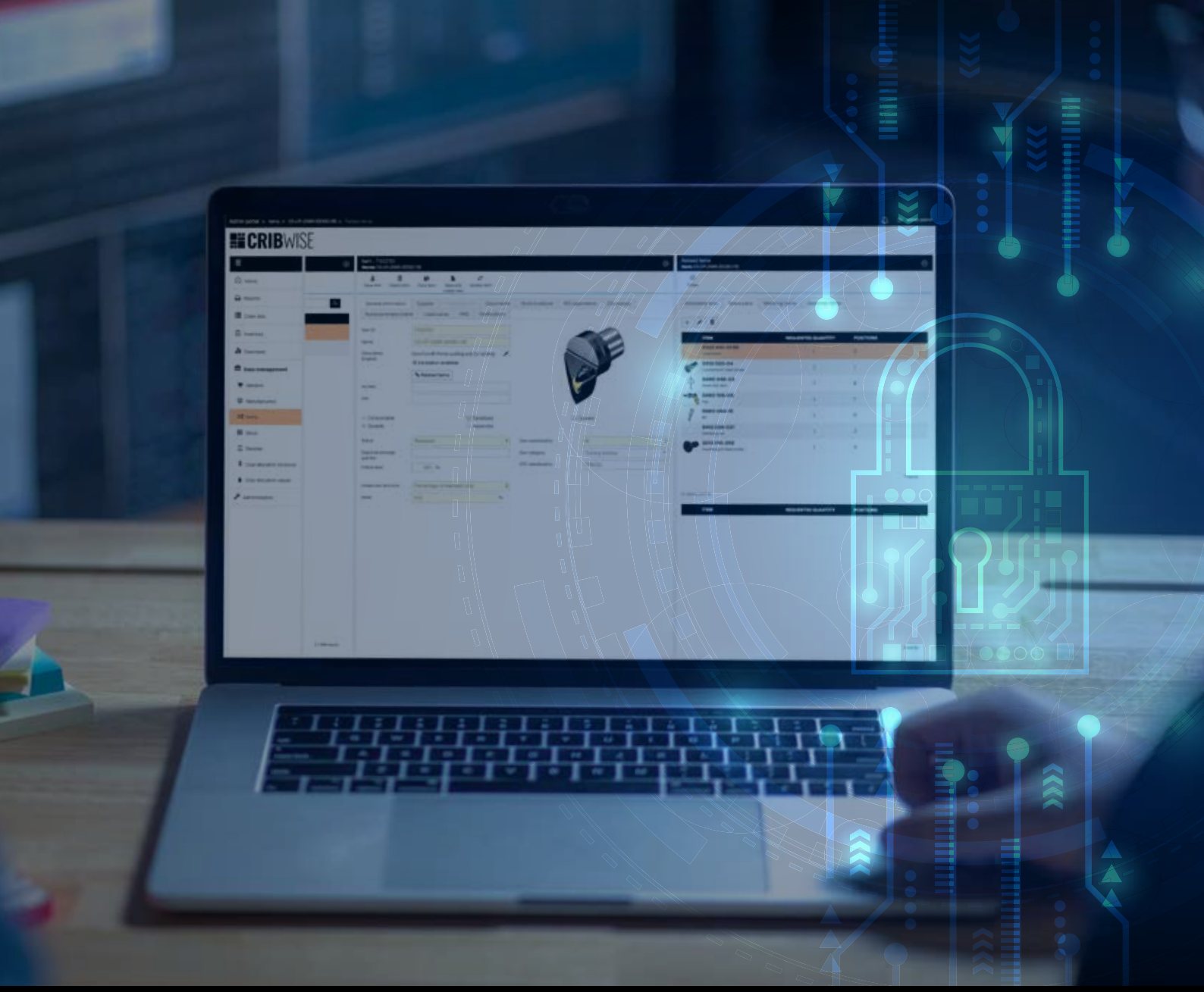


Cybersecurity for machine shops

A manufacturer’s guide to preventing supply chain attacks

CRIBWISE

Are you concerned about cybersecurity, hackers and data theft? Are these concerns preventing you from using the latest enterprise resource planning (ERP), inventory management software, and machine-monitoring systems? It is a common worry, but it need not be.

While your concerns should not be taken lightly, there are many simple, common-sense steps that you can take to protect the information and operational technology (IT and OT) that your machine shop relies upon. The security of the data held in cloud-based systems, meanwhile, can be managed expertly by their developers—allowing you to benefit from improvements in efficiency and productivity.

The costs of cybercrime

We should all take cybersecurity seriously. It is a myth that criminals only target large businesses; cybercrime can affect all businesses, both large and small. According to the Centre for Strategic and International Studies (CSIS), working in partnership with McAfee, as much as US$945 billion, a little over 1% of global gross domestic product (GDP), may be lost to cybercrime each year.[1] These attacks might be designed to steal intellectual property, or to cause disruption to a company's activities. The recent surge in supply-chain attacks, especially during 2021, shows an alarming trend in ransomware attacks that allow hackers to infect a high number of victims via automated software updates.

Limiting growth

As such, it is natural for you to be wary about investing in software and services that run on the Internet, instead of locally on your computer (so called cloud-based systems). After all, if you limit the exposure of your business to the Internet, you also limit your exposure to the criminals that inhabit it. You would, however, also be seriously limiting the potential of your business to grow. Such systems are an invaluable tool for improving the efficiency of your operations.

Further, most machine shops have already started to use monitoring systems that connect machine tools and other manufacturing equipment to local, shop-level networks, so that managers can keep track of production processes. These too are vulnerable to attack.

The reality is, however, that while cybercrime can be a threat to your business, there are a number of straightforward, common-sense steps that you can take on-site to protect your machine shop.

Providers of cloud-based software systems, meanwhile, will have dedicated cybersecurity teams that work tirelessly to protect your data and your manufacturing operations. CRIBWISE's Head of Cybersecurity, Design & Planning Automation, Elvira Cedergren, says: "The advantages of adopting cloud-based systems over legacy systems are numerous and compelling—both from security and productivity perspectives."

No solution will be 100% effective, but by doing the following, you can lower the risk from all but the most skilled, determined and tenacious of criminals.

Elvira Cedergren | Head of Cybersecurity, Design & Planning Automation

Strong passwords

When it comes to your on-site cybersecurity, start simple and remember the basics. Use strong passwords and DO NOT share passwords, a common practice in machine shops. Everyone should have their own username and password.

Simple and predictable passwords, and even those with numbers and symbols that appear to be complex, are easy for most cybercriminals to crack, if they so desire. Passwords with strings of sixteen or more characters can be generated randomly for added effectiveness.

The importance of education

Cyber criminals might target your computer systems, but your first line of defence should not be technology-based. It should be your people. You should train your staff to recognise the signs of a potential cyberattack. This alone will make your business more secure than most.

According to a recent survey, only 34% of those polled in the manufacturing sector thought core staff members took cybersecurity seriously.[2] The same survey found that just 31% of organisations said that their directors and top managers showed a very high commitment to cybersecurity.

People working in machine shops should know how quickly cyberattacks can shut down operations if they are not prevented. They should also know how to recognise common methods used by criminals, such as phishing emails (where fraudulent emails, text messages or telephone calls are used to trick victims into providing sensitive information), to harvest usernames and passwords to computers, and other sensitive data.

The good news is that there are myriad, freely available resources that can provide a good overview of cybersecurity for manufacturers. The NIST Cybersecurity Framework is a suitable place to start.

Protect your CNC machines

Map the existing computers and network infrastructure in your shop, and then start thinking in terms of risk. What can happen? Am I a target? What security measures do we need? Remember to consider all aspects of your shop – both the operations technology (OT) and the information technology (IT) – and think holistically so that you have all of the angles covered.

It is obvious that all of the mobile devices, laptops, PCs and servers in your network should be updated with the latest security measures, but what about your CNC machines? A malware could manipulate the programming of a machine so that it creates defective parts and, if the problem is not noticed in time, those parts could be sold and create danger for the people or companies using them. A hacked CNC machine could also be used to steal proprietary information.

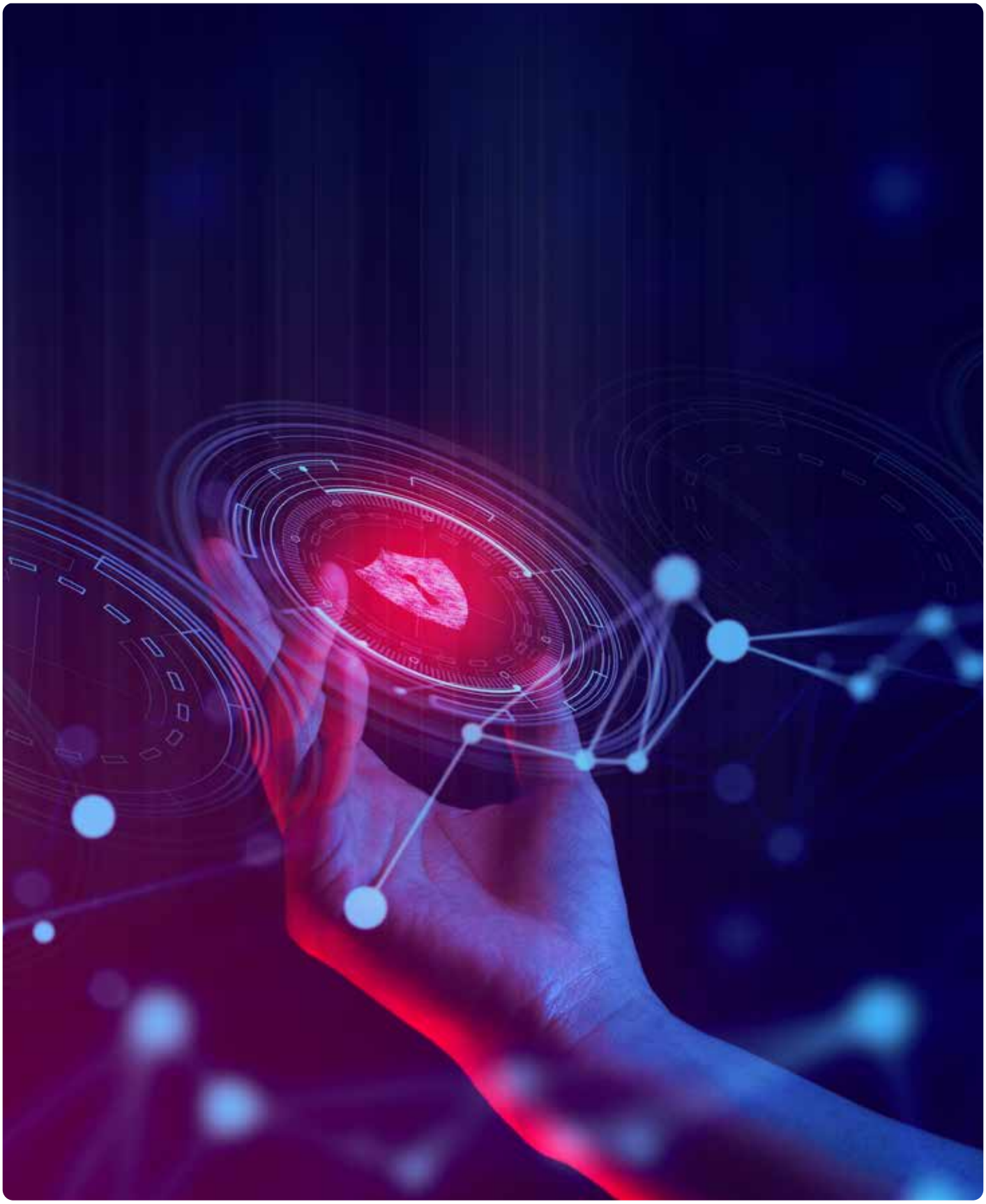
Machine shops can lock down their CNC tools, and other systems, by installing strong firewalls (barriers that sit between private computer networks and the Internet). It is also essential to use a strong authentication method between users, assets and tools that grant or deny access to their networks based on a set of rules for privileges. Also, keep operating systems and software updated, as security flaws in older versions will be well-known and easily exploited.

Network segmentation

Network segmentation is the practice of breaking larger networks down into smaller pieces, so that any security breaches can be isolated.

Think of the interior of a submarine, which is broken down into a number of compartments. Should the hull be breached, the adjoining compartment can be sealed, limiting flooding and preventing the vessel from sinking until repairs can be undertaken.

Network segmentation operates on a similar principal; a threat can be contained in a segment of a given network, so that it cannot move to other parts of an environment. Small security incidents can be quarantined, meaning organisations are better protected from breaches.



Plan for the worst

Develop a contingency plan that can be executed in the event of a breach of your cybersecurity. A contingency plan will help guide you and your staff so that you make the right decisions during a cybersecurity crisis. Without this plan, you could face additional attacks, take longer to recover and lose more money.

Develop a chain of command so that your employees know how to report an incident. Create and share a quick-response guide so that everyone in your organisation knows what to do in the event of a cyberattack. Back-up your data. Think about how you would communicate with your customers in the event of a data breach. Thinking about these things now will enable you to respond more immediately should the worst happen.

When it comes to your on-site cybersecurity, start simple and remember the basics. Use strong passwords and DO NOT share passwords.

Responsible vendors

There is much you can do to ensure your on-site security and providers of cloud-based software should have security resources that most businesses cannot maintain. Indeed, the reputations of these companies are built on state-of-the-art security they should provide.

To ensure that you buy your software from a vendor that really cares about your security, ask as many questions as you can during the procurement phase:

- Do they operate specific systems that automatically detect suspicious activity, and do they have dedicated teams in place that specialise in cybersecurity to combat attacks?
- Will your data be distributed across multiple servers in several locations, making it harder for cybercriminals to track-down confidential information?
- Will this data be backed-up and the back-up secured, so that – if the worst does happen – it can be recovered immediately and completely?
- Does the provider monitor, characterise, report and automate the logging of system activity and events?
- Does it detect and analyse intrusion attempts and work with its customers to investigate them?
- Does it frequently review, evaluate and update its software to fix weaknesses that could be exploited by the latest threats?

A responsible software company will not only be able to answer these questions for you in detail, but it will also take a great deal of pride in the levels of security it provides for its customers.

The CRIBWISE difference

At CRIBWISE, we have a dedicated team of cybersecurity professionals that works around the clock to ensure that our customers' data, and their businesses, are secure. CRIBWISE is modular, customisable and easy to integrate, and grants machine shops complete control over their tooling inventory with minimal effort and expense.

The software eliminates administrative hassles, eradicates production delays and cuts excessive (often hidden) expenditure.

CRIBWISE customers have reduced their inventory costs by as much as 20% and have cut their tool usage costs by up to 10%. On-hand inventory levels can be reduced by around 30%. When used to manage inventories of personal protective equipment (PPE), consumption of these items can be slashed by almost 40%.

To find out more about how CRIBWISE protects your data, and help you get control of your tooling inventory, please email us: help@cribwise.com

Machine shops can lock down their CNC tools, and other systems, by installing strong firewalls (barriers that sit between private computer networks and the Internet).

Sources:

1 https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

2 https://www.iotforall.com/iiot-cybersecurity-employee-training

CRIBWISE
Storviltsgatan 10
11542 Stockholm
Sweden

Phone: +46 (0)8 456 1100
Email: info@cribwise.com
Web: www.cribwise.com