CORVID

THE MOST BORING LIST MANUFACTURERS **MUST** READ

We get it – cyber security can be really boring. But ignoring it won't make the problem go away. Quite the opposite. Turning a blind eye to your cyber defences leaves your business vulnerable to state-sponsored and ransomware attacks.

To help you out, we've compiled a (mercifully short) list of the **top five critical cyber security mistakes manufacturers are making**, and what to do about them.

1 Complacency

Ask yourself if you've ever thought "a cyber attack will never happen to us". Large manufacturers may think they're safe because they have a cyber budget and IT staff, and small manufacturers may think they're too insignificant to be a valuable target. Wrong on both counts.

Your manufacturing company will be attacked, either directly or through a weak link in your supply chain. Whether it's a targeted, state-sponsored attack or an opportunistic drive-by, it's important to prepare your IT estate for compromise, so when the time comes, you can limit the damage to your operations, finances and reputation.

2 Insufficient backup

If you fall victim to a ransomware attacks and all your data is lost, could you get it back? Implement a rigorous backup schedule to ensure business-critical data can be retrieved. Store your backups in several secure locations, and make sure one of them is an 'offline' location that infected systems can't access.

Test your backups regularly to make sure they are being done correctly, and that your restoration procedures work as planned. You wouldn't want to discover they don't work after an attack has already stolen or blocked access to your files…

3 Reliance on reactive rather than proactive technologies

Sophisticated attacks bypass firewalls and anti-virus programmes – it's imperative to proactively hunt your IT estate for signs of compromise that have evaded these traditional methods. The longer an adversary has access to your network without being detected, the more damage they have time to do.

Email is the single biggest attack vector, so your email client needs the same level of proactive security. Some firewalls and email security solutions block senders who are known to be malicious, and remove certain types of attachments that are routinely used to initiate a compromise, before they reach your inbox.

If a malicious attachment is received and opened, application whitelisting will ensure only approved executables can run. You can also set up Microsoft Office to only allow macros from trusted sources.

Isolation sandboxing separates the malware from an email, before analysing and detonating it in a secure environment. If a user attempts to download ransomware (unknowingly or otherwise), it will never reach the network and your systems won't be affected.

4 Poorly configured systems that aren't kept up-to-date

Poorly configured environments can enable unauthorised access – it's imperative to ensure all systems are configured securely at all times.

Regular vulnerability assessments enable you to pinpoint weaknesses in your IT infrastructure that leave it susceptible to exploitation. The results of these can be used to define your detection and response capabilities, and determine if it's necessary to outsource your cyber security to a specialist provider.

Implement robust standardised builds for servers, workstations, laptops and other network infrastructure, to ensure comprehensive security across your entire network. As soon as new hardware is added, you can be confident it already has the appropriate security measures in place.

5 Expecting users to protect you from attacks

If your users are your first line of defence, your defences are going to succumb to attack.

Humans make mistakes. It's unrealistic and unfair to expect to successfully train users in complex IT processes, because they're not IT experts.

Invest in cyber security solutions that take your users out of the equation entirely, allowing them to get on with their day jobs without worrying about being responsible for a cyber breach.

DON'T MAKE IT EASY FOR ATTACKERS

Ensure your manufacturing company puts preventative measures in place to stop email-based attacks succeeding. **PERNIX** identifies and blocks malicious attachments, so the danger never reaches users' inboxes. They are then notified that malware has been removed and quarantined for their safety. PERNIX provides immediate email protection, without costly or complicated setup.

Want to see the difference it can make? **Get in touch with our experts** to request your free 30-day trial.

CALL US
+44 1242 651251

EMAIL US
contact@corvid.co.uk

VISIT US
www.corvid.co.uk

FIND US

CORVID

Arle Court, Hatherley Lane, Cheltenham, Gloucestershire, England, GL51 6PN