

---

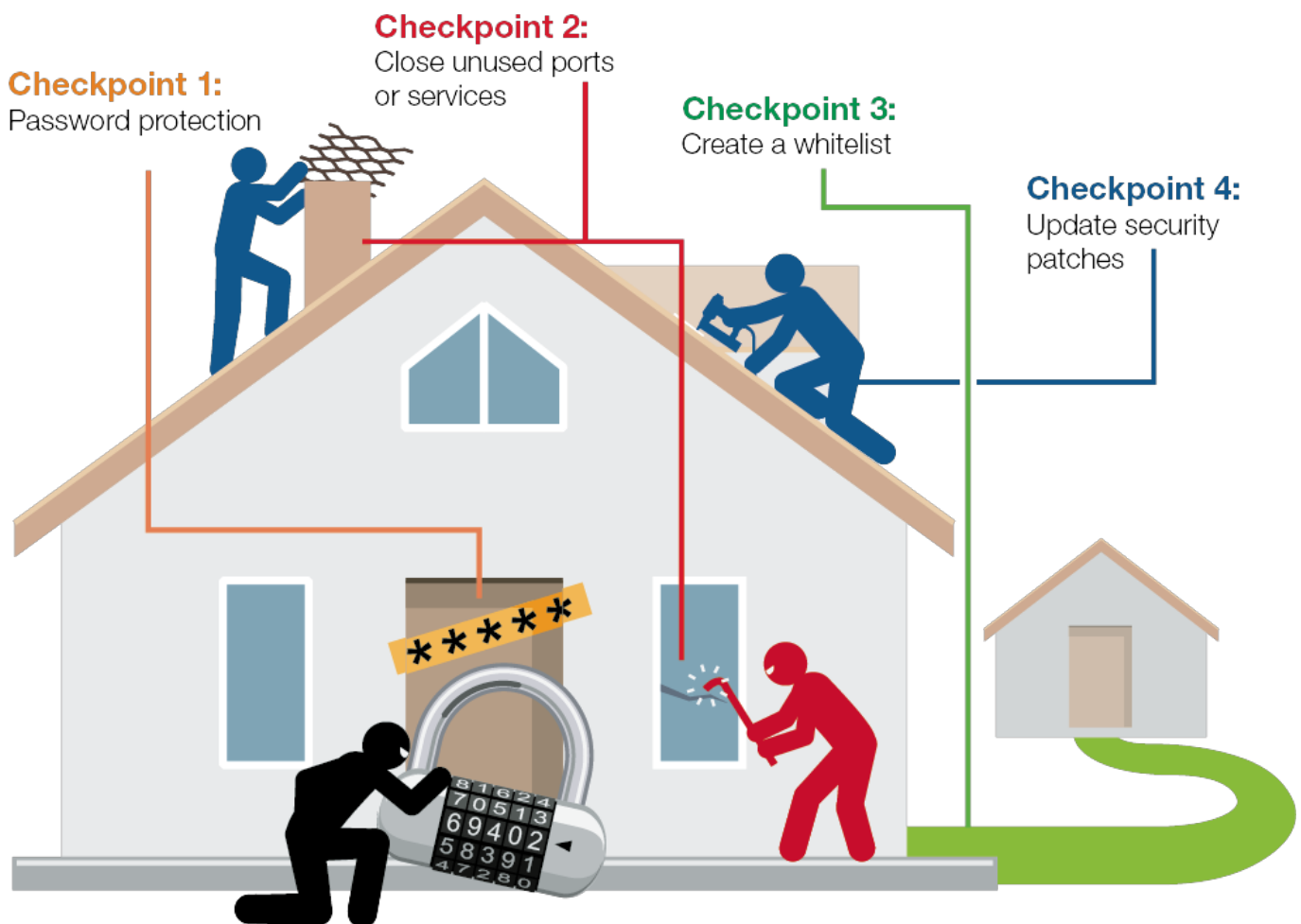
## Four Must-know Checkpoints For Beter Cybersecurity

Locking up our homes before we leave the house is second nature to us. Most of us don't even give this mudane yet conditioned task much thought although there are many good reasons for doing it. Apart from protecting our homes against the

elements of nature, we primarily want to keep unwelcome intruders out of our safe spaces. Nobody wants to come home to find it

damaged or valuables missing

---



**Data Theft a Major Threat to Companies**

---

The same rationale applies to the companies we work for. Owners would do everything possible to protect it from being damaged or against theft. These days, the theft of physical assets is not the only concern for company owners: Data theft has become a major headache. The ugly truth however is that in most workplaces cybersecurity measures are not as much prioritized as physical security measures. This lack of sufficient cybersecurity measures might come as a huge surprise, given the daily newsfeed of cyberattacks. For businesses to keep their business on a profitable track, an extensive review of their cybersecurity measures is vital if they don't want to pay the price for downtime caused by malicious attacks.

### **Big or Small, Everyone Is a Target**

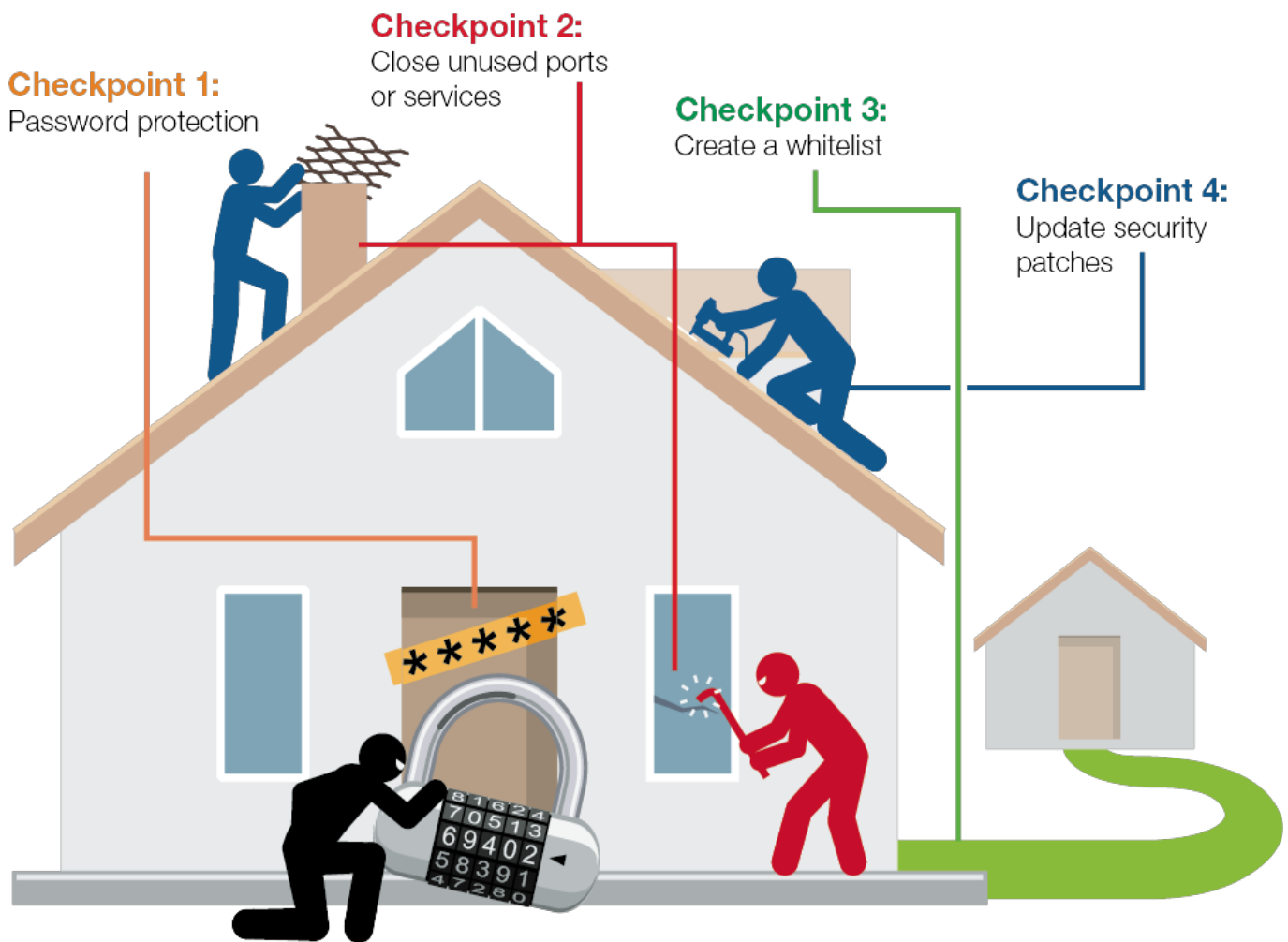
The assumption that a company is not a target based on its size or profile is a serious blunder, as a spike in cyberattacks has shown us that every business can be a target. For hackers any business asset, especially data, means money

Furthermore business owner need to change their mindset when it comes to managing cybersecurity, because it will never be a single product that provides protection ad infinitum. As long as cyberthreats keep morphing into different types of beasts cybersecurity will always be a continuous process of updating security measures and minimizing cybersecurity risks.

The good news is that business owners don't need to overcomplicate things when they want to ramp up their cybersecurity. Routine cyberhygiene practices can help you spot issues in the early stages in order to take the necessary action. For a well-maintained system to be less vulnerable to cybersecurity risks, proper tools or capable products are required for efficient cyberhygiene. The user and the solution provider are equally responsible to ensure the device and the network are secure

### **Prevention Is Better Than Cure**

As with our homes and families, a few sound precautions can make a huge difference. The following cyberhygiene checkpoints are essential to establish a secure connection for your field devices.



Checkpoint 1: Make sure the device is password protected and only allows authenticated users to access the system. You would be surprised how many devices are still keeping the default password for fast access, even though default account names and passwords can easily be obtained from the Internet by just a few mouseclicks. Good advice is to change your device password periodically.

Checkpoint 2: Reduce the surface areas for attacks. A service or a port in a device is like an open door or window in your house. Thus, having an unused service or port turned on is just as good as leaving a door wide open - a sign of welcome to any hacker out there. In order to reduce unexpected attacks, make sure all of your unused services or ports are turned off and allow real-time external connectivity only when absolutely needed.

Checkpoint 3: Create a whitelist for your access only. Only allow access and communication from specific devices and

connections. Clearly list the IP addresses that have authorization access to networking devices. Subsequently a majority of unauthorized IP addresses will be blocked

Checkpoint 4: Keep your security patches up-to-date. Security is not a one-time-fix: everyday there is a new virus being created or a new leak being discovered. Therefore it's essential to update the latest patches to prevent any new cyberattacks

## Moxa Solution

Moxa's serial-to-Ethernet solutions provide different security functions that meet your various cybersecurity requirements. If you are interested to find a serial-to-Ethernet device to secure your connection, you can download our checklist to implement industrial cybersecurity on serial-to-Ethernet devices or use the following table to find the product that suits you

| Product Category                                                                                                  | MGate Series <sup>1</sup>                                                                                               | NPort 5000/5000A <sup>2</sup>                                                                                           | NPort 6000                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <b>Login Authentication</b>   | <ul style="list-style-type: none"> <li>• Password protection (length, character enforcement)</li> </ul>                 | <ul style="list-style-type: none"> <li>• Password protection (length, character enforcement)</li> </ul>                 | <ul style="list-style-type: none"> <li>• Password protection (length, character enforcement)</li> <li>• Authentication servers (RADIUS/TACACS+)</li> </ul>                                  |
|  <b>Console Management</b>     | <ul style="list-style-type: none"> <li>• HTTPS (At least TLS 1.2)</li> <li>• Unused services can be disabled</li> </ul> | <ul style="list-style-type: none"> <li>• HTTPS (At least TLS 1.2)</li> <li>• Unused services can be disabled</li> </ul> | <ul style="list-style-type: none"> <li>• HTTPS (At least TLS 1.2 with the support of public certificate import)</li> <li>• SSH/SNMPv3</li> <li>• Unused services can be disabled</li> </ul> |
|  <b>Network Access Control</b> | <ul style="list-style-type: none"> <li>• Accessible IP List</li> </ul>                                                  | <ul style="list-style-type: none"> <li>• Accessible IP List</li> </ul>                                                  | <ul style="list-style-type: none"> <li>• Accessible IP List</li> </ul>                                                                                                                      |
|  <b>Vulnerability Scan</b>     | <ul style="list-style-type: none"> <li>• Perform Nessus Scan</li> </ul>                                                 | <ul style="list-style-type: none"> <li>• Perform Nessus Scan</li> </ul>                                                 | <ul style="list-style-type: none"> <li>• Perform Nessus Scan</li> </ul>                                                                                                                     |

