5 Cybersecurity Questions You Must Ask Yourself

What keeps you awake at night as a security professional? We believe that these five cybersecurity questions, if left unanswered, will develop into much larger issues.

1. What assets do we own?

Of all the cybersecurity questions to ask yourself, the first step in any security risk management programme is being aware of your assets. Typically, an attacker will go for the path of least resistance, which is often that dusty old server tucked away somewhere that's been long forgotten. If you don't already have an asset register for IT equipment, start one.

It really doesn't need to be anything too intensive: just a list of each item of equipment, where it's located physically, where it's located on the network (host names & IP addresses), plus which member of staff is accountable for it. If you already have an asset register, make sure there is a process in place to maintain it and keep it up to date.

2. What are our security vulnerabilities?

Next up in our list of cybersecurity questions, you must figure out the security vulnerabilities present in each of your assets and, more importantly, figure out the level of risk that the vulnerability presents to your organisation. Not all vulnerabilities are created equal, and the risk they present to your business depends on the impact of a successful exploit (i.e. what sensitive data or functionality would be exposed?) as well as the likelihood of an attack. For example, if the asset isn't connected to a network then the likelihood of a successful attack is massively reduced.

Managing all this information long-term can be a scary prospect. So, maintain a risk register alongside your asset register. This documents the known risks to a given asset, as well as the intended actions to address the risks.

Many security vulnerabilities can be resolved through vendor-supplied security patches. So check systems regularly for missing security patches. Operating System vendors often provide (free) tools to perform automated checks. For example:

- Security Patch Check for HP-UX; or
- Microsoft Baseline Security Analyzer (MSBA) for Windows.

A next step would be to run a vulnerability scan. These often incur a yearly license fee but they do identify additional security vulnerabilities introduced by configuration flaws. Nessus is a good option, as is Qualys.

Automated vulnerability scans are always worthwhile and should form part of a 'defence in depth' approach to security. However, according to WatchGuard, "30% of malware attacks are zero-day exploits that cannot be identified by legacy antivirus systems because they have not been seen in the wild before".

This means additional, manual penetration testing should be considered for all critical applications, networks and devices.

3. Do our people know what makes good password security?

It sounds simple, because it is. The latest Verizon Data Breach Investigations Report states that 81% of hacking-related breaches are the result of either weak or stolen passwords. So, update your passwords periodically. Make sure they're suitably complex, made up of multiple character sets and the longer the better. Even better, opt for 'passphrases', which are longer and more complex, but easier to remember than a long random list of characters.

A password manager will help generate and retrieve these, as they store your passwords in an encrypted database. A great example is LastPass.

When storing passwords, make sure they're salted wherever possible. A salt will add additional data to your password hash. This makes it immune to decryption using pre-computed Rainbow Tables (which attackers regularly use to retrieve plain-text passwords stored without hashes in seconds)

A hacker will attempt to crack a salted hash but the longer and more complex your password the more time it's going to take trying to crack it.

4. Who holds the 'Keys to the Kingdom'?

Do you use the "Principle of Least Privilege"? Administrative user groups such as Domain Admins in Windows networks have full access to all data within your network. Wherever possible, restrict the use of these highly privileged user accounts and operate on a need-to-know basis.

5. Do we operate on a flat network?

Don't rely on a single line of defence when it comes to information security. Instead build 'Defence in Depth', using multiple layers of defence to prevent a single point of failure.

Always operate under the assumption that something will be compromised at some point in the future .

The issue with a flat network from a security point of view is that traditional filtering controls won't necessarily be available, because there are other devices sitting on the same subnet. Due to this, compromise of a single server or workstation would place the entire network at risk.

Where possible, segment your network into multiple subnets. Every business is different, but as an example, place your users' workstations in a different network segment to your database servers. That way, if one of your users was to get fooled by a phishing email, the more critical data stored in your databases wouldn't immediately be at risk.

In Summary

You can make huge progress by implementing small steps and without it costing the earth.

We know security vulnerabilities are a concern but there doesn't need to be a mass panic; if we can advise each other in areas that we have immediate control over then our organisations could be much more secure.

We've listed the areas that we feel are most relevant here at Secarma; ones that can provide a great deal of protection if actioned properly.

Secarma can help you stay secure

We believe that the security of your critical networks and data is key to your organisation's success. Whatever your sector, whatever your size, our mission is to help you to seize the competitive advantages of providing your clients with security, compliance, and reliability.

Got any more cybersecurity questions? Our experts are here to answer your queries and put you on the right path towards advanced security maturity. Contact a member of our dedicated team today.