Developing a Cybersecurity Strategy to Protect End-Users

www.Centaris.com

The creation of an effective cybersecurity strategy should be a priority for all businesses.

You only need to look at recent security breaches to see why. They affect everyone — from giant corporations to government agencies to small, independent organizations.

Attacks are common — and the strategies used are becoming increasingly sophisticated. This means the cybersecurity landscape is constantly evolving as attackers find more innovative and effective ways to target their victims.

If your business is still relying on traditional methods to deal with and prevent cyberattacks, it's time for an upgrade. Outdated security not only puts your business at risk, but it also puts your end-users at risk. Here's why you need to focus on people to make sure you're ready to deal with any threats that come your way:

Cybersecurity: Why We Need to Focus on People

Firewalls, anti-virus software, and encryption can only do so much. If the people working in your organization don't understand your cybersecurity policies — and how to protect themselves from cyberthreats — the risk to your business increases significantly, despite any other preventative methods you're using.

This is because hackers are increasingly targeting people when they attack.

It’s a strategy that makes a lot of sense when you consider the hacker must find weaknesses in your organization to exploit. People are an easy target because it only takes one simple, unintentional mistake to let the cybercriminals in.

For example, according to Verizon’s data breach investigations report, 94 percent of malware was delivered via email. Often, these emails are almost indistinguishable from legitimate communications. This makes it difficult for the people working in your organization to recognize them as a threat — unless you have risk management strategies in place to both educate and protect them.

> **“94 percent of malware was delivered via email.”**
>
> – Verizon

As well as installing malicious software through email communications, hackers may target individuals within your company directly when attempting to gain access to your systems.

Who Are the High-Risk People Within Your Business?

To understand which people are most at risk within your business, you need to think like an attacker.

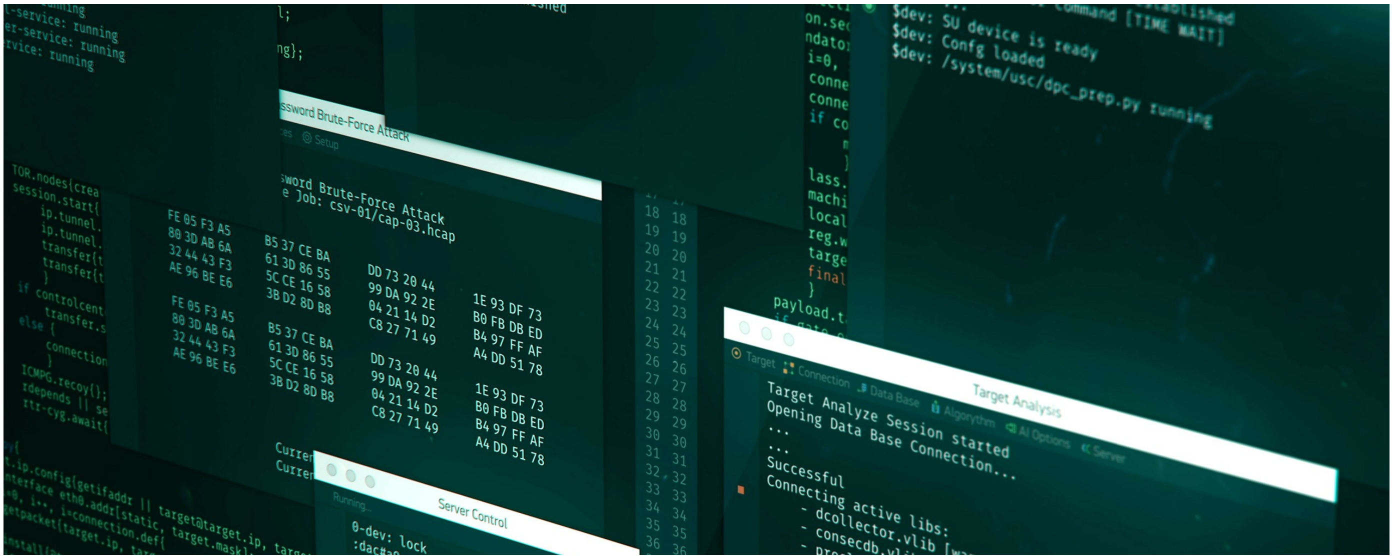
When someone attempts to hack into your organization’s computer systems, they’re doing so for a reason. It could be that they want to access customer data, which they plan to sell on to a third-party. Or it could be that they’re trying to access sensitive information (e.g. in the case of corporate espionage).

Whatever the reason, they target the people within your business who can give them what they want. This means people with access to sensitive data, customer information or company secrets.

The CEO, directors and their assistants are obvious choices. These people often have access to high-level information, as well as customer data.

Engineers and IT staff are also high-risk as they tend to have access to a variety of systems, both physical and digital, that appeal to hackers. Gaining access to these systems may enable the attackers to gain access to the sensitive data we’ve already mentioned, as well as to take actions to disrupt the business (e.g. install malicious code, delete data, damage systems).

Finally, anyone who works remotely, away from the organization’s physical location, poses an additional risk.



What Are the Factors That Contribute To End-User Risk?

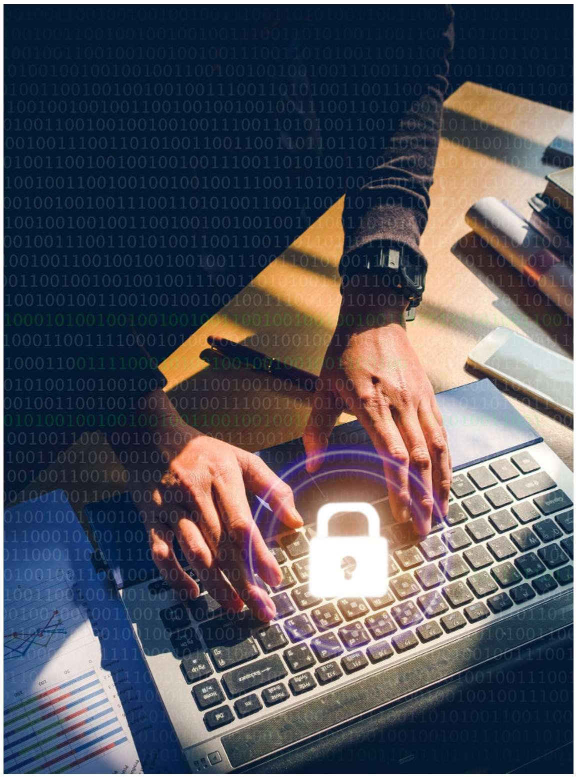
There are many factors that influence the risk posed to end-users and your business. These include:

- **Vulnerabilities** – for example, outdated software that hasn't been kept up-to-date is likely to have weak points attackers can exploit.

- **Access rights** – users that have access to privileged information are at risk as this increases the likelihood the users have access to something the hackers want.

- **Knowledge** – if an end-user doesn't know how to keep themselves (and your business) safe, how can you expect them to do it? While some data breaches are caused by negligent staff, many arise simply because the appropriate policies, procedures, and training aren't in place.

Understanding these factors is key to risk mitigation.



How to Mitigate Risk and Reduce Attacks

When it comes to mitigating your risk and reducing cybersecurity attacks on your business, focusing on the enduser is an essential part of a successful cybersecurity strategy.

Here are a few ways you can do this:

Document the Relevant Policies and Procedures

A good starting point is to ensure all relevant policies and procedures are documented, easily accessible, and introduced to new staff starting at the business.

These should be easy to read and understand — and displayed in locations across the business to remind employees as they go about their work.

Educate Your Staff

The policies and procedures won't mean much if your staff hasn't received adequate training.

Develop sessions on cybersecurity to walk your employees through the actions you expect them to take to keep themselves and your business safe.

Make sure they know how they pose a threat to your business and the kind of threats they need to look out for.

Refresh Their Knowledge Regularly

The cybersecurity landscape is evolving constantly. You need to ensure your employees understand this and keep up-to-date with the changes they'll need to make as attacks get more sophisticated.

Leave all your employees with no doubt about the roles they need to play to prevent an attack.

Change Passwords Regularly and Keep Software up to Date

These both seem so simple, but cybersecurity strategies don't have to be complicated.

Simple actions, such as requiring mandatory password changes once per month, can make all the difference when it comes to mitigating the risks posed by cybercriminals.

What will you do to keep your end-users safe?

Contact Us

www.Centaris.com

248-284-7100

36333 Mound Road, Suite C
Sterling Heights, MI 48310