Cyber Security

The EDFR NA Cybersecurity Team

Jonathan Alexander
Director, Cybersecurity

Kevin Brown
Manager, Cybersecurity

Ryan McLean
Sr Cybersecurity Engineer

Mick Legge
Cybersecurity Analyst

Ryan Hicks
Cybersecurity Analyst

edF renewables

Cyber Security
Protect | Detect | Respond

Cybersecurity Defined

So what exactly is Cybersecurity?

Cybersecurity is the state or process of protecting and recovering computer systems, networks, devices, and programs from any type of cyberattack.

Some specific duties include:

- Monitoring the network to identify any irregular activity
- Perform audits to ensure security practices are compliant
- Deploy endpoint detection and prevention tools to block malicious hacks
- Review the security viability of applications or vendors
- Set up a vulnerability management system across all assets on-premises and in the cloud
- Educate employees on how to identify suspicious activity.

There are very few aspects of our daily lives that network-based technology does not touch. Wherever those interactions occur there is risk. Employees equipped with the knowledge and resources needed to improve their cyber-IQ is one of the easiest ways to reduce that risk. That's why cybersecurity is a shared responsibility!

Cybersecurity in Our World

No one can deny that now more than ever technology runs our lives. No longer is it just smartphones and laptops, now Internet-of-Things (IoT) devices such as refrigerators, watches, televisions, front doors, and even garages are network connected.

That connection means that all these devices are possible vectors for cybercriminals to attack and they can come from anyone on the planet with an email account and access to the internet.

Some recent statistics show the effect this proliferation has had globally.

- There is a hacker attack every 39 seconds.
- There are 375 new security threats created by minute.
- In the last three years the number of phishing websites has increased by over 130%.
- IoT devices experience an average of 5,200 attacks per month.
- Roughly 92% of malware is delivered via mail.
- Americans lose $15 billion annually to identity theft.

Cyber Crime
damage costs to hit
$6 trillon
annually by 2021

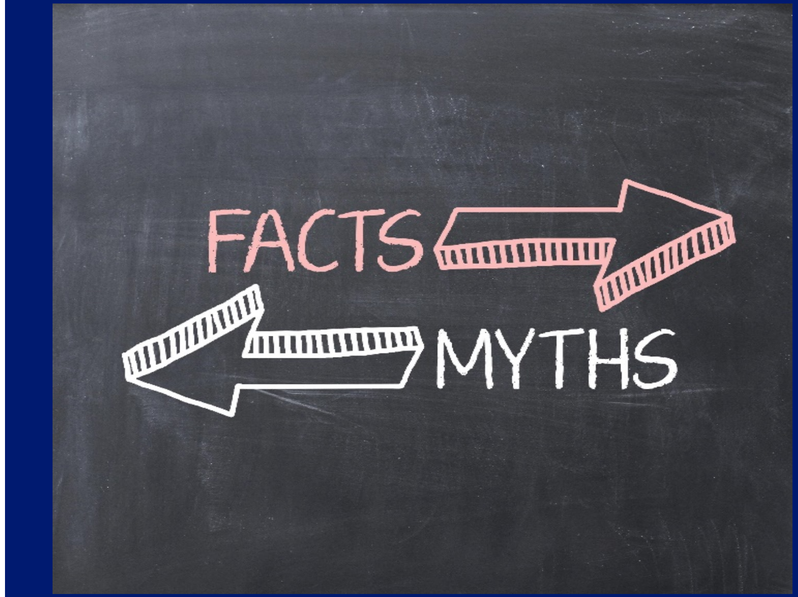
Cybersecurity as a Culture

- There is a seemingly insurmountable flow of threats and there is no silver bullet solution so what can we do? It starts with the understanding that we all have a role in establishing a culture of security whether at the office or working remotely.
- We know some attacks are bound to be successful. Even the best technical solutions will miss one now and then, just based on the volume we see daily.
- Having a workforce that is knowledgeable about what these attacks may look like and how to respond to them increases the likelihood that any damaging effects can be kept to a minimum or avoided altogether.

Many myths that have plagued the topic of cybersecurity over the years which have had a detrimental effect on overall security and safety cybersecurity practitioners hope to maintain.

- A strong password is enough to keep me safe.
- Most cyber threats only come externally.
- If there is a password on a Wi-Fi network, it's secure.
- Antivirus is all I need to accomplish complete security.
- Hackers only target large corporations.
- My data isn't valuable, so it doesn't need to be protected.

Cybersecurity



edF renewables

Having a complicated password is an important part of protecting your online persona – but it shouldn't stop there.

Myth 1:
A strong password is enough security

Facts:

- Changing your password every 120 days reduces your chance of being hacked and exposure to danger.
- Using strong and unique passwords for every single account, you have online will make it more difficult for a hacker to use the same username and password on your other accounts.
- You should use a password manager to keep track of all your passwords if they are too unique to remember, or you are changing them regularly.
- Use of two-factor authentication is the most effective means of protection. Even if your password is cracked or stolen a hacker would still need to somehow get your second means of authentication.

While we hear more about outside hackers breaching organizations that is not the only method. A cyberattack can come from someone working at our organization right now or from someone working at one of our vendors right now.

Myth 2: Cyber attacks only come from external sources

Facts:

- Protecting the physical location of servers can reduce the risk of theft or tampering.
- Educating employees on the essential security measures to take when handling sensitive documents or information online is critical.
- Using the concept of least privilege and assigning role-based access can limit damaging effects.

Although it is more difficult to hack a public Wi-Fi connection with a password, there are still vulnerabilities to be aware of and ways to protect yourself while travelling for work.

Myth 3: A password on a public Wi-Fi makes it secure

Facts:

- Anyone using the same public Wi-Fi connection can perform a man-in-the-middle attack between your laptop and the router, slip malware onto your computer or create fake hotspots that look like real networks to connect to.
- Only visit websites with HTTPS at the beginning of the URL as this encrypts the data and makes the connection more secure.
- Using the VPN (virtual private network) will route your internet traffic to a server that the company owns, which will stop intruders from seeing your information.

Just because you have an antivirus product installed on all your devices doesn’t mean that you’re protected against malware of every type.

Myth 4:
Antivirus is all I need for protection against malicious software

Facts:

- If the endpoint protection isn’t properly maintained, it can be vulnerable to the latest iteration of malware.
- Cybercriminals change methods quickly so even the most sophisticated patchwork of antivirus, anti-spyware, firewalls, and intrusion detection can’t stop all attacks.
- Keeping an eye out for reports of security failures that pertain to any product or service you use can provide a great deal of security benefit.

Huge corporations and big-name businesses that get hacked make the news most often, and so it can seem like only big companies are being targeted.

Myth 5:
I'm too small to be a target for attackers

Facts:

- Cybercriminals are always seeking out small businesses and individuals with ties to larger ones in hopes of getting access to the larger companies.
- For example, hackers once breached a small HVAC service company and gained access to all the credit card data in a major retailer's point-of-sale system.
- With the amount of money to be gained there is not a single entity with a tie to the internet that doesn't have a target.

Myth 6: I don’t have any data to protect so I don’t need to worry about security

Most people misjudge the value their data has on the illegal market.

Facts:

- Seemingly insignificant data can be used by attackers. It may not be your data attackers are after, but they can use information they gather to go after larger targets.
- Personally Identifiable and Protected Health Information are often mishandled by employees &/or vendors.
- An audit and classification should be done for all the data you create, collect, store, access, or transmit to ensure it has the proper protections according to its sensitivity.

Cybersecurity at Home

Working from home is the new norm. Here are some tips to stay safe and secure in this socially distanced workforce.

- Avoid mixing work and leisure activities on the same device. Activities such as Facebook, Instagram, etc. should be done on personal devices due to the increased risk they can introduce.
- Ensure your home Wi-Fi is secured using strong Wi-Fi encryption such as WP2 and a strong unique password for access; and by changing the Wi-Fi router admin password from the default.
- The Virtual Private Network (VPN) on your company laptop should never be turned off. If you have an issue with VPN contact Support Services.
- Have a list of IT contacts to call in the event of an IT emergency.
- Social engineers have stepped up their tactics – spoofing senders and even sending texts that look alarmingly legitimate. As a rule of thumb – be wary of any correspondence you did not initiate and report any that don't pass the sniff test.

Cybersecurity SharePoint

The EDFR Cybersecurity Department has a SharePoint Online site that will be used as the go-to portal for all things related to security with the organization. Including:

- Security policies
- Request templates
- Links to Wire articles
- Glossary of security terms
- Security tips and how-tos

We are adding more content so check back from time to time or you can even contact the team and provide input about things you might like to see. Cybersecurity email account – infosec2@edf-re.com

Click here to access