precision CYBERTECHNOLOGIES & DIGITAL SOLUTIONS

CYBER DIGITAL WORLD

NEWSLETTER

Volume 2: Issue No. 2 **October:** 2021

Dr. Ronald Walcott
Managing Director

In our last issue, we indicated that October is cybersecurity awareness month. As such, we continue to provide information on this critical and important topic.

WHY IS CYBERSECURITY PARAMOUNT?

Data leaks are becoming more and more common, allowing sensitive information to land in the hands of the wrong people. 2021 is not yet over, but more than 180 million people have already been on the receiving end of a data breach.

These breaches can negatively impact businesses and their customers, and can result in:

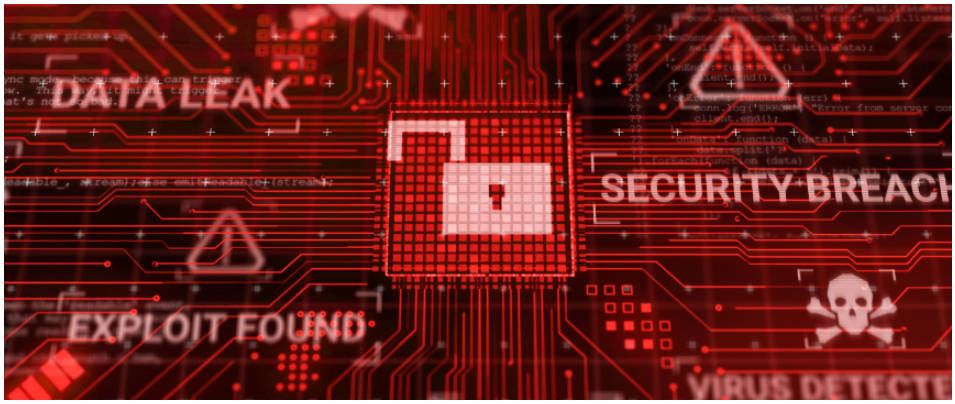
- Credit card fraud
- Criminal activities
- Significant revenue and sales losses
- Law suits
- Fines and other issues

Cybersecurity is serious! Having proper systems in place can help businesses and individuals to protect themselves from the negative impact of cyber-attacks.

Source: https://www.analyticsinsight.net/

Do You Know How Much Your Digital Information is Worth?

Information is where data is synthesized into something useful. In business today much emphasis is placed on data gathering and analytics, as companies compete for market share.



The path to adequate cyber protection begins with understanding your information assets and the impact of Confidentiality, Integrity and Availability.

WHAT IS AN INFORMATION ASSET?

An information asset can be described as information or data that is of value to the organization, including such information as patient records, intellectual property, or customer information. These assets can exist in physical form or electronically.

Whether your organisation is large or small, if you do not understand your information, you cannot fully protect it. Assessing every individual file, database entry or piece of information as an information asset isn't practical, actually, it is more

In this Issue:

effective to group information into manageable portions.

An information asset is defined at a level of granularity that allows its parts to be managed usefully as a single unit: if it's too broad you will not have enough detail, if it's too fine, you will have thousands of assets.

ASSESSING INFORMATION ASSETS:

To assess whether something is an information asset, ask the following questions:

- Does the information have a value to the organisation?
- How useful is it?
- Will it cost money to reacquire?
- Would there be legal, reputational or financial repercussions if you couldn't produce it on request?
- Would it influence operational efficiency if you could not access it easily?
- Would there be consequences of not, having it?
- Is there a risk associated with the information?
- Is there a risk of losing it? A risk that it is not accurate? A risk that someone may try to tamper with it? A risk arising from inappropriate disclosure?
- Does the group of information have a specific content? Do you understand what it is and what it is for? Does it include the entire context associated with the information?
- Does the information have a manageable lifecycle?
- Were all the components created for a common purpose?
- Will they be disposed of in the same way and according to the same rules?

CYBERSECURITY MYTHS THAT YOU NEED TO KNOW

Below are six common myths about cybersecurity, with focus on small business:

Myth #1: My Business Is Too Small to Be a Cyber Target.

Reality: Any business can be a target. In 2018, 43% of all data breaches hit small businesses, according to the Verizon 2019 Data Breach Investigations Report. Why? Unfortunately, many small businesses don't keep up with cybersecurity best practices and this makes them easy targets..

Myth #2: I Don't Sell Products on my Website, so I Don't Need to Worry.

Reality: Whether you sell online or not, you still need website security. There are two major reasons for this: 1., without proper malware protection, your site could be hacked and vandalized by attackers so that when prospective customers browse your website, they see random or offensive messages instead of information about your business. 2. , if your site lacks SSL protection, you could be at risk for easy attack.

Myth #3: We don't Have Anything Worth Stealing.

Reality: You just might! , There are several reasons why hackers may choose to go after small businesses instead of multinationals, big banks and other large corporations These reasons include:. Holding your business hostage. Ransomware attacks make the news when they disrupt cities and big businesses, but small businesses are frequent targets, too. In 2018, an estimated 70% of ransomware attempts went after small businesses. The typical ransom for owners to get their data back and get their business up and running again was on average US$116,000. (THIS CONFLICTS WITH INFO LISTED LATER ON, WHICH USES A FIGURE OF 140,000.... SUGGEST TO USE ONE FIGURE FOR CONSISTENCY)

Myth #4: Our Stuff Is Password-Protected, so We're Good.

Reality: As counteless hacks and breaches have shown, Passwords aren't fool proof.. Passwords work if they can't be cracked. But most passwords are easy to figure out, either by guessing or with a bot that keeps trying combinations until it gets a match. It is recommended that businesses ensure that employees use strong passwords as an added layer of protection.

Myth #5: My Employees and I Know How to Spot a Phishing Email.

Reality: Phishing attempts are a lot harder to detect than a few years ago- e-mails are not always the medium used.

In the past, phishing was characterised by poorly worded e-mails, some of which blatantly asked for money. However, more recently, , text and voice messages appear to come from customers, utility providers or vendors. Some asks for money, arising from "past due" bill payments, sensitive data, or may ask for you to click on a link that lets ransomware into your system.

Myth #6: Setting Up Your Cybersecurity Is a One-Time Event and Costly.

Reality: Criminals are always finding new ways to steal information, so cybersecurity best practices are always adapting and evolving. It's sound business to keep up with the latest security news and keep educating yourself and your employees. It's also essential to have security tools that operate 24/7 to monitor your business data.

HEADLINE NEWS:

Ransomware: Average Ransom Payment Stays Steady at $140,000

When a business, government agency or any other organization gets hit by ransomware and opts to pay a ransom to its attacker in exchange for a decryption key or some other promise, on average it pays $140,000.

So says ransomware incident response firm Coveware, based on thousands of incidents it investigated for the period July through August.

In a news report detailing Q3 trends, Coveware says that the average ransom payment remained largely steady, compared to Q2, while the median increased by more than 50%.

This shift, it says, started after a number of high-profile attacks that began in May, including DarkSide disrupting U.S.-based Colonial Pipeline, causing consumers to panic-buy fuel. Not long after, REvil - aka Sodinokibi - attacked meat processing giant JBS, and over the Fourth of July holiday weekend, there was an attack on the remote management software firm Kaseya, whose software is , used by managed service providers and small to medium businesses. , security

The attacks sparked a furious political response from the Biden administration and other governments, galvanizing international efforts to target ransomware attackers via law enforcement, disrupt cryptocurrency flows to eat away at profits, and focus on improving the cybersecurity resilience of domestic businesses. The White House has also been increasing diplomatic pressure on Moscow to crack down on cybercriminals operating from inside Russia..

Apparently, in response to the fallout, DarkSide ceased operations, rebranding as BlackMatter. REvil went offline in July for unexplained reasons, before resurfacing in September. The same month, security firm Bitdefender received the keys from law enforcement officials that enabled it to build and release a free decryptor for almost all REvil infections pre-dating from July. In October, , REvil's infrastructure went offline again, with an administrator claiming operators pulled the plug after someone hijacked REvil's Tor-based data leak and payment portal sites.

Source: Ransomware: Average Ransom Payment Stays Steady at $140,000 (databreachtoday.com)

Frequently Asked Questions:

WHAT ARE THE MAIN CAUSES OF BREACHES?
95% of cybersecurity breaches are caused by human error.

HOW MANY CYBER ATTACKS HAPPEN DAILY?
On average 2,244 attacks happen per day!

WHAT ARE THE TOP MALICIOUS EMAIL ATTACHMENTS?
The top malicious email attachment types are .doc and .dot which make up 37%, the next highest is .exe at 19.5%

HOW MUCH PERSONAL DATA HAS BEEN BREACHED?
Personal data was involved in 58% of breaches in 2020

WHAT IS THE AVERAGE RANSOMWARE PAYMENT?
The average ransomware payment rose 33% in 2020 over 2019, to $111,605.

Upcoming Events

CYBERSECURITY SUMMIT: NEW YORK
November 9, 2021

VIRTUAL CYBERSECURITY SUMMIT INDIA & SAARC: ZERO TRUST
November 16, 2021

VIRTUAL CYBERSECURITY & FRAUD SUMMIT: FRANCE
November 23, 2021

Source: https://www.databreachtoday.com/events

868-610-7237
salesinfo@precision-cyber.com
www.precision-cyber.com
1st Floor, Brair Place, 10-12 Sweet Road
St. Clair, Port of Spain, Trinidad