precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume: 15 November 2022

Today, we are focusing on the importance of good cybersecurity as it relates to business continuity.

Dr. Ronald Walcott
Managing Director

Ever since the invention of the internet, computers, phones, tablets and other devices that have network connectivity, cybersecurity has become more and more of a focal point for small, medium and large businesses, as well as government organizations. While in the Caribbean there may be a lower frequency for cyberattacks when compared to other parts of the world, the rate at which these attacks are occurring has been rapidly increasing to a worrying level. Many businesses in the Caribbean region are yet to implement good cybersecurity practices such as:

- Training and educating employees on good cybersecurity practices (eg. Frequent changing of passwords & using strong passwords).
- Implementing and enforcing policies to protect assets (eg. Restrict access to files, devices, etc using passwords).
- Installing antivirus, protective software, implementing firewalls, network policies, etc.
- Monitoring network traffic and patterns.

If businesses and organizations don't have these things in place, it can mean that attackers can gain access to and have control of sensitive information that could potentially decommission a business and completely shut down their operations. However, if a business does have these things a place the likeliness of the business being able to continue to operate and suffer less losses would be significantly higher.

WHAT IS BUSINESS CONTINUITY PLANNING?

Business continuity planning (BCP) is the process of creating preventative and recovery systems to deal with potential cyber threats to an organization. The plan considers many internal and external factors and aims to ensure process continuity in the event of a cyberattack. BCP also has a secondary goal. This goal is to ensure operational continuity before and during the execution of a disaster recovery plan. The BCP planning entails the protection of assets and personnel. Simply put, the basic requirements of a BCP are to have the essential business functions running and available during a disaster, while recovering with the least amount of downtime and losses as possible.

WHY IS BUSINESS CONTINUITY IMPORTANT?

For many organizations, it is 100% unacceptable for their services and products to be unavailable for ex-

In this Issue:

tended periods of time. Business continuity is critical for organizations to address client management, retention and operational security. If a business' essential functions are disabled for a period of time, it could mean losing out on the opportunity to gain income or losing money. A robust BCP is essential for companies to ensure that key functionality being disabled doesn't have crippling consequences and so that they can resume functioning like normal in the shortest period of time while simultaneously mitigating financial risks.

STEPS IN BUSINESS CONTINUITY PLANNING

Conduct Business Impact Analysis & Risk Assessment -
Risk Assessment involves identifying the risks to the company, analyzing those risks and evaluating the risks to determine how significant the risks are and if it falls into the acceptable risk levels.

Develop Recovery Strategy
This is the plan of action that is developed to regain functionality after a disaster or attack that disrupts the normal flow of business.

Implementation of Solution
Identifying the best plan option and executing it.

Testing & Acceptance
At this step, the business tests how effective the solution they have implemented is. This is done from using various tests, such as vulnerability testing and or penetration testing.

Routine Maintenance
At this stage, the businesses improve and fix any kinks in their armor that may leave them vulnerable to risks that could affect their continuity.

HAVING BUSINESS CONTINUITY PLAN VS NO BUSINESS CONTINUITY PLAN EXAMPLE OF BCP

Ireland's healthcare industry had been the target of a ransomware attack in 2021. The attack had widespread effects on operations.

- IT outages affected at least 5 hospitals.
- Employee payments were knocked offline, delaying pay for 146,000 staff
- Near full restoration and recovery of all servers and applications took more than 3 months.
- The attack cost more than $100 million in recovery efforts alone.

However, Ireland had a BCP and disaster recovery plan in place, so they were able to mitigate and reduce their risks by:

- Cybersecurity teams shut down 85,000 devices to stop the spread of malware.
- Disaster recovery teams inspected more than 2000 IT systems one by one to contain damage and ensure they were clean.

Here we see how critical a BCP and Disaster Recovery Plan is because even though there was a BCP and disaster recovery plan in place, the industry still suffered severe losses and full functionality took a long time to be restored. If there was nothing in place, what then? Imagine the scale of losses that would have been suffered.

Upcoming Events

CYBERSECURITY & CLOUD EXPO
December 1st - 2nd, London, UK

BLACK HAT EUROPE -
December 5-8th 2022, London, UK

MISSION CRITICAL: SECURING CRITICAL INFRASTRUCTURE, CONNECTED DEVICES, AND CRYPTO & PAYMENTS
December 13th, 2022

Frequently Asked Questions:

ARE BCPS AND DISASTER RECOVERY PLANS COSTLY?

The cost of BCPs can vary depending on the level of risk that a company thinks is acceptable. This will determine the amount of investment the company may need for the level of preparedness and responsiveness they desire.

IF A BCP AND DRP DOESN'T STOP THREATS COMPLETELY, WHY IS IT IMPORTANT?

They are important because it reduces the likelihood of an attack completely crippling the business and significantly reduces the amount of time that is taken to be fully functional again.

References

ROCK, T. (2022, MARCH 14). 7 REAL-LIFE BUSINESS CONTINUITY EXAMPLES YOU'LL WANT TO READ.
Retrieved November 24, 2022, from Invenio IT website: https://invenioit.com/continuity/4-real-life-business-continuity-examples/

BUSINESS CONTINUITY PLANNING. (2020, DECEMBER 31).
Retrieved November 24, 2022, from EC-Council Logo website: https://www.eccouncil.org/business-continuity-planning/

Headline News:

Firms Spend $1197 Per Employee Yearly to Address Cyber-Attacks

Companies pay an average of $1197 per employee yearly to address successful cyber incidents against email services, cloud collaboration apps or services and browsers.

Security researchers at Perception Point shared the findings with Infosecurity before publishing them in a new white paper this month.

According to the new data, the above figures exclude compliance fines, ransomware mitigation costs and losses from non-operational processes, all of which can cause further spending.

The survey, conducted in conjunction with Osterman Research in June, considers the responses of 250 security and IT decision-makers at various enterprises and reveals additional discoveries regarding today's enterprise threat landscape.

"These findings demonstrate the urgent need for organizations to find the most accurate and efficient cybersecurity solutions which provide the necessary protection with streamlined processes and managed services," commented Perception Point CEO Yoram Salinger.

Among the findings is that malicious incidents against new cloud-based apps and services occur at 60% of the frequency with which they take place on email-based services.

Additionally, some attacks, like those involving malware installed on an endpoint, happen on cloud collaboration apps at a much higher rate (87%) when compared to email-based services.

The Perception Point report also shows that a successful email-based cyber incident takes security staff an average of 86 hours to address.

In light of these figures, the security company added that one security professional with no additional support can only handle 23 email incidents annually, representing a direct cost of $6452 per incident alone.

Conversely, incidents detected on cloud collaboration apps or services take, on average, 71 hours to resolve. In these cases, one professional can handle just 28 incidents yearly at an average cost of $5305 per incident.

"The rapid growth of non-email-based threats crucially underscores the need for security teams to keep up with emerging trends," added Salinger, "especially as the modern work environment is in flux and the number of cloud-based collaboration tools that organizations rely on is only likely to expand."

The Perception Point white paper's publication follows a separate report by JumpCloud published last week suggesting cybersecurity-specific funding might be at risk.

Source: www.infosecurity-magazine.com