NETWORK BOX
NEXT
GENERATION
MANAGED SECURITY

www.network-box.com

In the Boxing Ring DEC 2023

Network Box Technical News

from Mark Webb-Johnson
Chief Technology Officer, Network Box

Welcome to the December 2023 edition of In the **Boxing Ring**

Season's Greetings, and best wishes for the festive season! This month, we conclude our **Understanding Company's Security Posture** series. Today, businesses increasingly rely on technology and digital infrastructure. While this offers numerous benefits, it also exposes businesses to potential risks and disruptions - no business of any scale is immune to cyberattacks. Thus, ensuring a robust security posture is paramount. On pages 2 to 3, we discuss the importance of having a disaster recovery plan, and why your business may be a target for hackers.

In other news, we are proud to announce that Network Box Singapore SOC is now certified by TÜV SÜD PSB Pte Ltd. according to **ISO 27001** - many congratulations to our Singapore team! In addition, Network Box USA, together with MSP Toolkit and Praxis Data Security, hosted a live cybersecurity event. Finally, Network Box Hong Kong welcomed students and faculty from Raimondi College's Infomation and Communication Technology department to a cybersecurity seminar/workshop.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
December 2023

Stay Connected

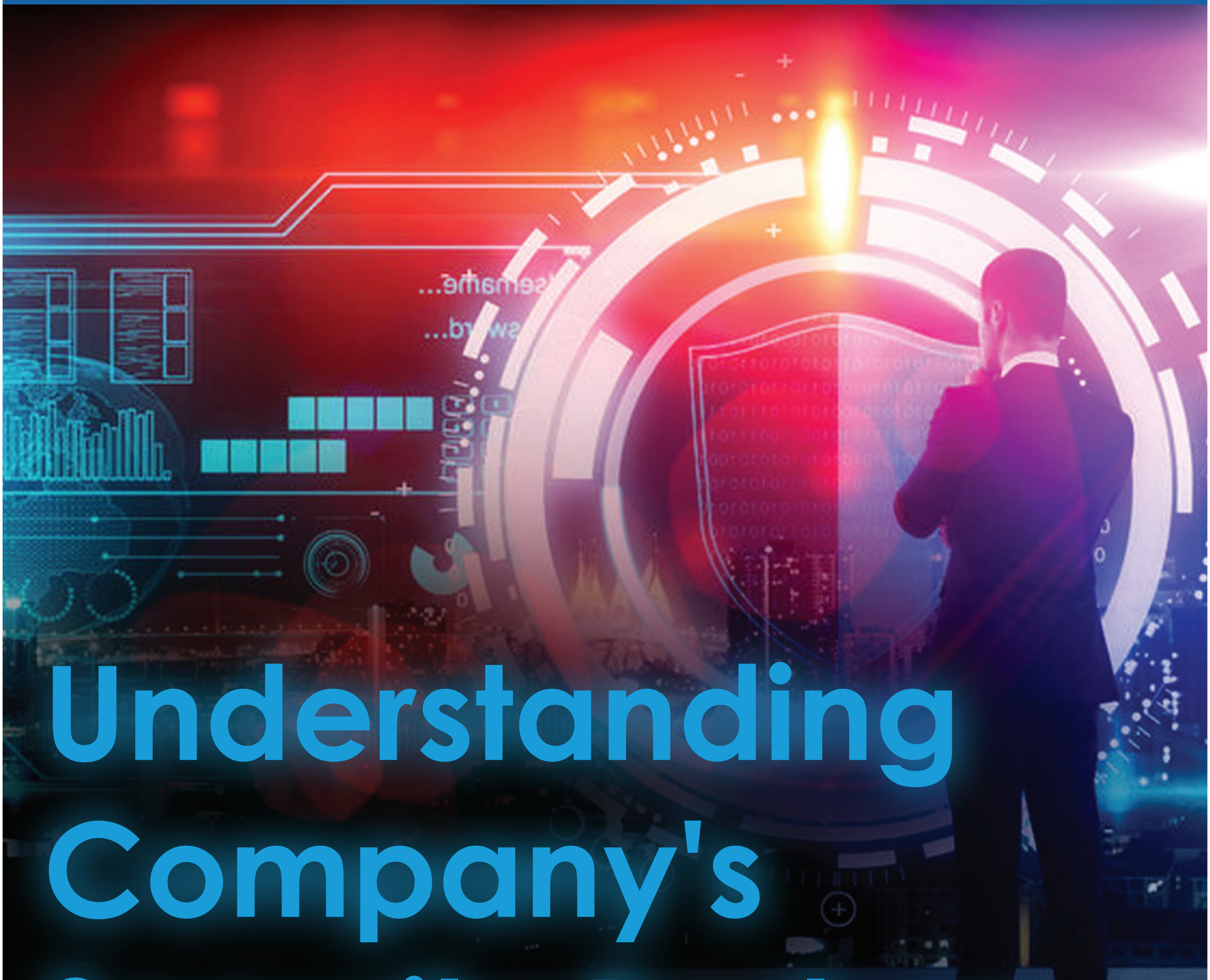
You can contact us here at Network Box HQ by email: **nbhq@network-box.com**, or drop by our office next time you are in town. You can also keep in touch with us by several social networks:

https://twitter.com/networkbox

https://www.facebook.com/networkbox
https://www.facebook.com/networkboxresponse

https://www.linkedin.com/company/network-box-corporation-limited/

https://www.youtube.com/user/NetworkBox



Understanding Company's Security Posture (part 2)

by Kseniia Degtiareva
Network Box Cybersecurity Consultant

Today, businesses increasingly rely on technology and digital infrastructure. While this offers numerous benefits, it also exposes businesses to potential risks and disruptions. Thus, ensuring a robust security posture is paramount. In this article, part two of our Security Posture series, we will discuss the importance of having a disaster recovery plan and why your business may be a target for hackers.

Why you need a disaster recovery plan

Disasters, both natural and non-natural, can severely impact business operations. As such, businesses must have a well-defined disaster recovery plan in place to mitigate its negative consequences. A disaster recovery plan is a defined set of processes and procedures that outline how an organization will respond and recover from various disasters. It ensures critical business functions can be restored quickly and efficiently, minimizing downtime and reducing financial losses.

The following are some key reasons why businesses need to have a disaster recovery plan in place:

Minimizing Downtime and Loss of Productivity: Disasters can cause significant disruptions to business operations. Without a proper recovery plan, businesses may struggle to get back on track, leading to extended downtime, loss of productivity, and potential revenue loss. A well-prepared disaster recovery plan ensures that necessary measures are in place to minimize downtime, allowing businesses to resume operations as quickly as possible.

Protecting Data and Information: Data is one of the most valuable assets for businesses today. Data can be compromised or lost entirely, leading to severe consequences for a business. A disaster recovery plan should include backup and recovery procedures to safeguard critical data and information. Thus ensuring data can be restored and accessed efficiently to protect the integrity and continuity of business operations.

Ensuring Business Continuity: Disasters can have long-lasting effects on a business if not properly addressed. A disaster recovery plan enables businesses to maintain continuity during and after a disaster. It outlines the crucial steps to ensure essential functions can continue, even in adverse circumstances. By prioritizing business continuity, organizations can minimize the impact of disasters on their operations and maintain the trust and confidence of their customers.

Meeting Regulatory and Compliance Requirements: Many industries have specific regulatory and compliance requirements regarding data protection and business continuity. A robust disaster recovery plan helps businesses meet these requirements and comply with applicable laws and regulations. Businesses can demonstrate their commitment to protecting sensitive information and maintaining operational integrity by having a disaster recovery plan.

A disaster recovery plan is critical to any business's risk management strategy. It provides a roadmap for mitigating the impact of disasters and enables businesses to recover swiftly and efficiently. By investing in a well-designed and regularly tested plan, businesses can protect their operations, data, and reputation, ensuring long-term success in an unpredictable world.

Is your business a target for Hackers?

In today's cyber threat landscape, no business of any scale is immune to cyberattacks. Hackers constantly scan the Internet for vulnerable targets, and businesses of all sizes can become victims. Here are a few reasons why hackers would target your business:

Valuable Data: The potential for financial gain often drives hackers. Your business becomes an attractive target if you deal with valuable data, such as customer information, payment details, or intellectual property. Hackers can exploit this data for various malicious purposes, including identity theft, financial fraud, or selling it on the dark web.

Industry Reputation: Specific industries are more prone to cyberattacks due to the valuable information they hold. For example, healthcare organizations store sensitive patient data, financial institutions handle large sums of money, and technology companies possess valuable intellectual property. Hackers may target businesses in these industries to gain access to valuable information and exploit their reputation for financial gain.

Weak Security Measures: Hackers often look for the path of least resistance. If your business has weak or outdated security measures, it becomes an easy target. This includes using weak passwords, not regularly updating software, lacking proper encryption, or neglecting employee cybersecurity training. Hackers can exploit these vulnerabilities to gain unauthorized access to your systems and data.

Ransomware Potential: Ransomware attacks have become increasingly prevalent in recent years. Hackers use malicious software to encrypt your business's data and demand a ransom for its release. Any business can become a target of ransomware, especially if they have valuable data and weak security measures in place.

Competitive Advantage: In some cases, hackers may target businesses seeking a competitive advantage. Competitors or individuals with malicious intent may attempt to gain unauthorized access to your business's proprietary information, trade secrets, or upcoming product plans. By doing so, they aim to gain a competitive edge or disrupt your business operations.

> **Businesses must understand that cyberattack threats are real and can have severe consequences. Implementing robust cybersecurity measures, regularly updating security patches, and educating employees about best practices can significantly reduce the risk of being targeted by hackers. Remember, cybersecurity is an ongoing endeavor. Stay vigilant, stay informed, and protect your business from the ever-evolving cyber threat landscape.**

Network Box HIGHLIGHTS

Network Box Singapore
ISO/IEC 27001 : 2013 Certification

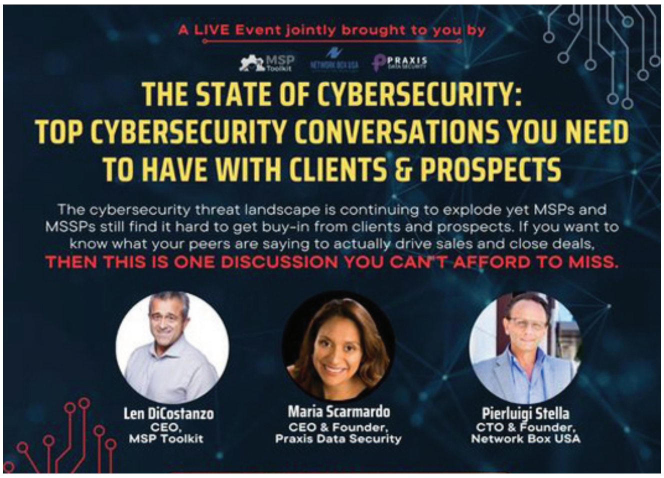
Network Box is proud to announce that our office in Singapore, Network Box (SIN) Pte Ltd, is certified by TÜV SÜD PSB Pte Ltd. according to **ISO 27001**. Meaning, Network Box Singapore Security Operations Centre has established and applies an Information Security Management System for the installation, configuration, monitoring, and support of Network Box Unified Threat Management Appliances.

TÜV SÜD ISO 27001

CERT NO.: IS27-2023-0192
ISO/IEC 27001 : 2013

Network Box USA
Cybersecurity Live Event

Network Box USA, together with MSP Toolkit and Praxis Data Security, hosted a live event titled ***"State of Cybersecurity: Top Cybersecurity Conversations You Need to Have with Clients & Prospects."*** Covering various topics including: Compliance, Frameworks, Risk, SASE, XDR, SIEM, AI/ML, Edge Defense, IAM, DLP, Ransomware, and Cyber Insurance.



A LIVE Event jointly brought to you by

MSP Toolkit · Network Box USA · PRAXIS Data Security

THE STATE OF CYBERSECURITY:
TOP CYBERSECURITY CONVERSATIONS YOU NEED TO HAVE WITH CLIENTS & PROSPECTS

The cybersecurity threat landscape is continuing to explode yet MSPs and MSSPs still find it hard to get buy-in from clients and prospects. If you want to know what your peers are saying to actually drive sales and close deals, THEN THIS IS ONE DISCUSSION YOU CAN'T AFFORD TO MISS.

Len DiCostanzo
CEO,
MSP Toolkit

Maria Scarmardo
CEO & Founder,
Praxis Data Security

Pierluigi Stella
CTO & Founder,
Network Box USA

Network Box Hong Kong
Cybersecurity Seminar

Network Box Hong Kong welcomed students and faculty from **Raimondi College's** Infomation and Communication Technology department. The seminar highlighted the current cyber threat landscape and technologies available to mitigate these threats.

Newsletter Staff

Mark Webb-Johnson
Editor

Michael Gazeley
Kevin Hla
Production Support

Network Box HQ
Network Box USA
Contributors

Subscription

Network Box Corporation
nbhq@network-box.com
or via mail at:

Network Box Corporation
16th Floor, Metro Loft,
38 Kwai Hei Street,
Kwai Chung, Hong Kong

Tel: +852 2736-2083
Fax: +852 2736-2778

www.network-box.com

Copyright © 2023 Network Box Corporation Ltd.