NETWORK BOX | NEXT GENERATION MANAGED SECURITY

www.network-box.com

In the Boxing Ring OCT 2023

Network Box Technical News

from Mark Webb-Johnson

Chief Technology Officer, Network Box

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

This month, Network Box's Managing Director, Michael Gazeley, discusses **Why Government Legislation is Imperative for Strengthening Cybersecurity.** Technology has become integral to our everyday lives, from mobile phones to laptops and desktops, to smart devices such as CCTVs, refrigerators, and webcam-equipped televisions. However, with cyber threats constantly evolving, posing significant risks to individuals, businesses, and even national security, it is critical for governments to enact legislation to tackle these issues head-on.

In other news, Network Box participated in the **Servereye Partner Day** which took place at the Big Eppel Culture and Congress Center in Eppelborn, Germany. Additionally, Network Box has been listed as one of the top providers in the **Cloud Intrusion Detection and Prevention Market Report**. And in this month's global security headlines, there were security issues with **Cisco**, **Juniper**, **Google**, and **Linux**.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
October 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

In this month's issue:

STRENGTHENING CYBERSECURITY: why government legislation is IMPERATIVE

by Michael Gazeley
Managing Director
Network Box Corporation

The need for robust cybersecurity measures cannot be overstated in today's hyper-connected world, where technology has become an integral part of our everyday lives. From our omnipresent mobile phones to our laptops and desktops, to smart devices such as CCTVs, refrigerators, and webcam-equipped televisions, which rule our day-to-day existence - everything is an internet-connected computer now. With cyber threats constantly evolving, posing significant risks to individuals, businesses, and even national security, it is critical for governments to enact legislation to tackle these issues head-on.

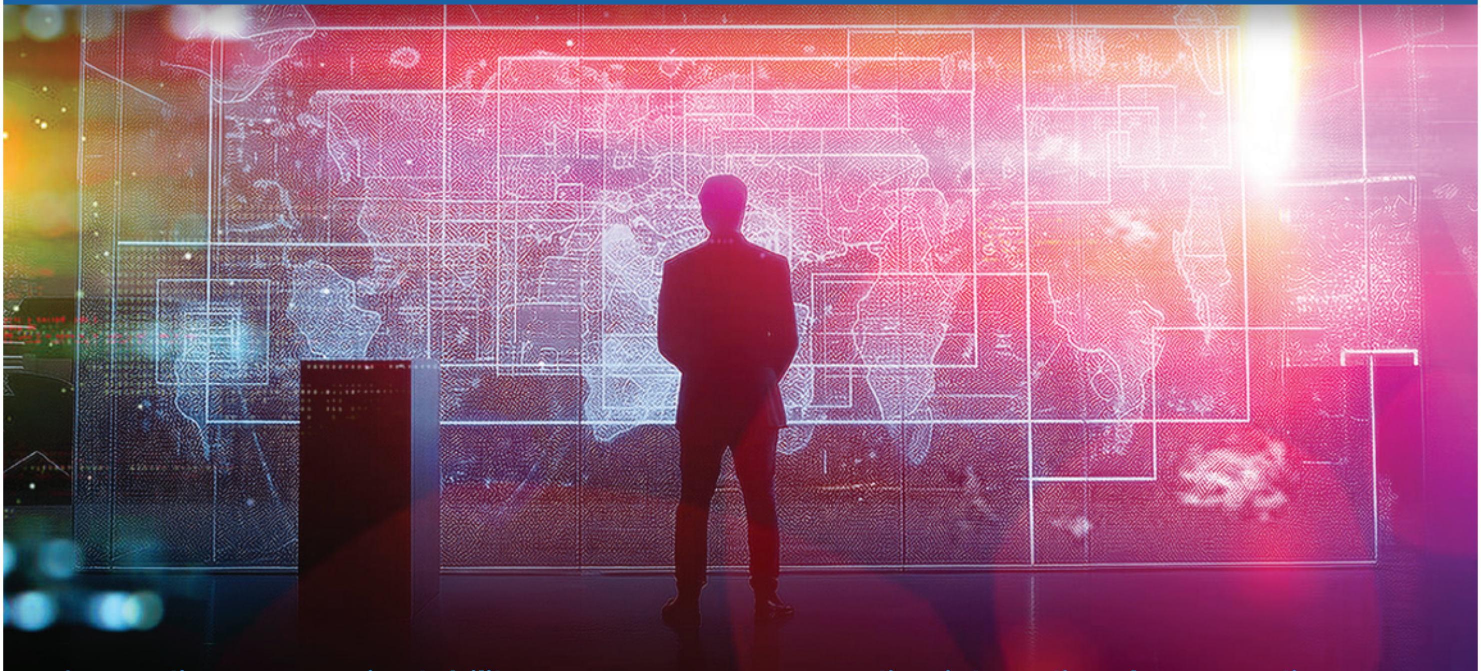
Given the objective failure of organizations to secure themselves from hackers and malware, government legislation on cybersecurity is necessary, bringing potential benefits to society as a whole. Just look at the number of confidential credentials posted on the Dark Web by hackers, which stands at 12.6 billion and counting. There are more hacked accounts than there are people on Earth. **If that is not a call to action, I don't know what is.**

Safeguarding personal information

In this digital age, personal data is constantly at risk of being compromised. Yet governments and organizations force us to give up more and more of our information. We often have no choice but to fill in the online forms presented to us, typically with the exact information a hacker can use to steal our identities. Identity theft, financial fraud, and unauthorized access to private information have become alarmingly common. Government legislation on cybersecurity can empower individuals by instituting standards and regulations to protect personal information. Implementing robust data protection laws, such as stringent encryption protocols and mandatory breach notification requirements, can significantly reduce the risk of data breaches and protect citizens from the potential consequences of cybercrime.

Educating and enhancing public awareness

With the rapid advancement of technology, cyber threats are continuously evolving, necessitating ongoing education and awareness initiatives. Government legislation in cybersecurity can facilitate the implementation of public awareness campaigns, educational programs, and training opportunities to increase citizens' cyber literacy. Helping citizens become aware of the tactics used by cybercriminals is imperative. By promoting responsible digital practices and equipping individuals with the skills to protect themselves online, government legislation can empower citizens to navigate the cyberspace securely, ultimately reducing susceptibilities to cyberattacks. Artificial intelligence is also bringing a whole new level of threat, as what we see/hear/believe is being challenged with ever more sophisticated deep fakes.



Supporting economic stability

Cyber threats not only jeopardize individuals' privacy but also pose a significant risk to our economies. Businesses of all sizes, from multinational corporations to small startups, are increasingly vulnerable to cyberattacks that can result in financial losses, reputational damage, and even bankruptcy. Government legislation, in the realm of cybersecurity, can foster a secure environment for businesses to thrive. Governments can provide businesses with the necessary tools to safeguard their digital assets and ensure economic stability by mandating adequate cybersecurity measures and promoting information sharing about emerging threats. For governments to implement threat intelligence and install 'cyber radar' to monitor threats in real-time, would make all the difference to ongoing economic stability.

Protecting national security

Cyberattacks now have the potential to disrupt essential services, compromise sensitive government information, and even threaten national security. By legislating cybersecurity, governments can establish comprehensive frameworks to protect critical infrastructure, safeguard classified data, and respond effectively to cyber threats that may originate from internal and external sources. This proactive approach allows governments to counteract potential attacks and reduce the impact on the nation's security. The first blow to a nation's security, even in the case of a war commencing, is far more likely to come from a targeted cyberattack than a barrage of cruise missiles. Indeed, modern warfare now includes the use of hackers and malware, as much as tanks and aircraft. The biggest threat to a nation or an economy is likely the use of an enemy's cybersecurity equipment during a time of peace, only for that equipment to become a Trojan Horse if and when a war, or even a cold war, commences.

Promoting international cooperation

Cyber threats are not confined within national borders; they are a global concern. Government legislation on cybersecurity creates a foundation for international cooperation in combating cybercrime. On a non-military, law enforcement level, global collaboration can help the entire world combat cyber criminals much more effectively. By establishing international standards and frameworks, governments can collaborate with other nations to address cross-border cyber threats more effectively. This approach will facilitate information sharing, joint investigations, and the extradition of cybercriminals, ultimately leading to a safer and more secure cyberspace on a global scale. In the end, there is only one Internet to police, despite that Internet existing across some 206 economies. This means securing the Internet needs to be done collectively. It is simply impossible for one country or economy to do it all alone.

> **The urgency to prioritize cybersecurity has never been greater, with cyber threats escalating in complexity and severity. New malware, vulnerabilities, and hackers appear all the time. They target our identities, our assets, and even our core beliefs. Unfettered attacks on societies can, and unfortunately do, result in a world where not even what is fact and what is fiction is clear anymore. Facts matter. Truth matters. The government's role in legislating cybersecurity cannot be underestimated. Leaving all of this to companies, organizations, and private individuals just doesn't work. By enacting comprehensive cybersecurity legislation, governments can protect national security, safeguard personal information, support economic stability, promote international cooperation, and educate the public about the importance of cyber resilience. Through these measures, governments can create a safer and more secure digital environment for individuals, businesses, and nations. The time to act is now, and through collaborative efforts between governments, industries, and citizens, we can build a resilient cyber infrastructure that protects us, empowers us, and propels us forward into a secure digital future.**

Network Box HIGHLIGHTS

Network Box Germany
Servereye Partner Day

Network Box Germany participated in the Servereye Partner Day, which took place at the Big Eppel Culture and Congress Center in Eppelborn, Germany. The theme of the event was "Together High" and Network Box Germany provided a workshop on security awareness.

Global Security Headlines

GBHackers
Cisco IOS Verification Flaw Let Attackers Execute Arbitrary Code
LINK: https://bit.ly/48BAJ6X

Bleeping Computer
Thousands of Juniper devices vulnerable to unauthenticated RCE flaw
LINK: https://bit.ly/468tamA

Bleeping Computer
Google assigns new maximum rated CVE to libwebp bug exploited in attacks
LINK: https://bit.ly/3ET5AhH

Dark Reading
Akira Ransomware Mutates to Target Linux Systems
LINK: https://bit.ly/48w0Dc5

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

Cloud Intrusion Detection and Prevention Market by Development Factors 2031

Network Box has been listed as one of the top providers in the Cloud Intrusion Detection and Prevention Market Report.

LINK: https://bit.ly/3RCRqbQ