

Payment Card Industry Data Security Standard (PCI-DSS)

Overview & Compliance

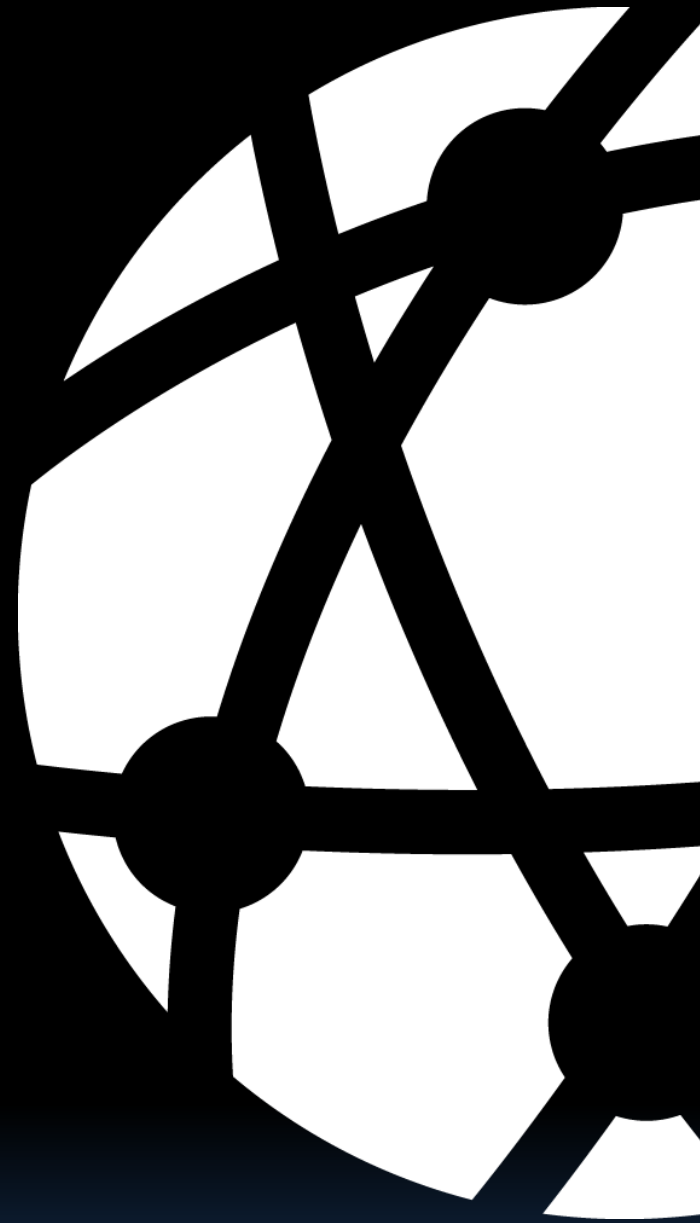
Jan van Leersum
Network Box Singapore
Managing Director

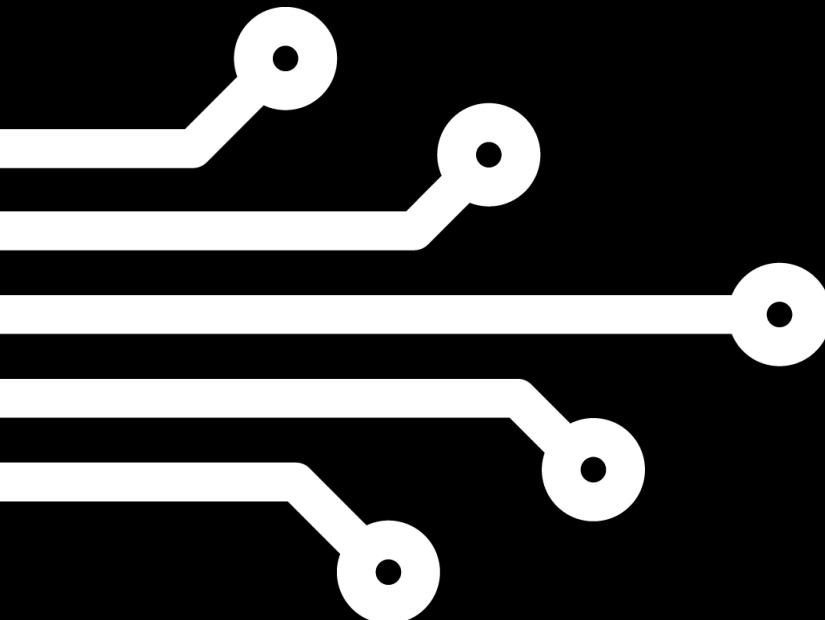


Retail Cyber-Risk Landscape Overview

**When you
plug into the
world,**

it's easy to forget
the world is also
plugged into **YOU**



A series of white lines on a black background, resembling a circuit board or network diagram. The lines start from the left and branch out to the right, ending in small white circles.

The Internet has
revolutionized how
the retail industry
does business, and
has become a 'must'
for all

Yet, businesses in the
retail industry are still
reluctant to protect
themselves effectively.

About $\frac{1}{5}$ Data breach
incidences are
from the
RETAIL industry

11.3 million

accounts were hacked from electronic toy manufacturer, **VTech**. Data stolen included photos and personal details of children.

vtech



TARGET®

110 million

personal data, and credit card details
stolen from US retail giant, **Target**.

233 million

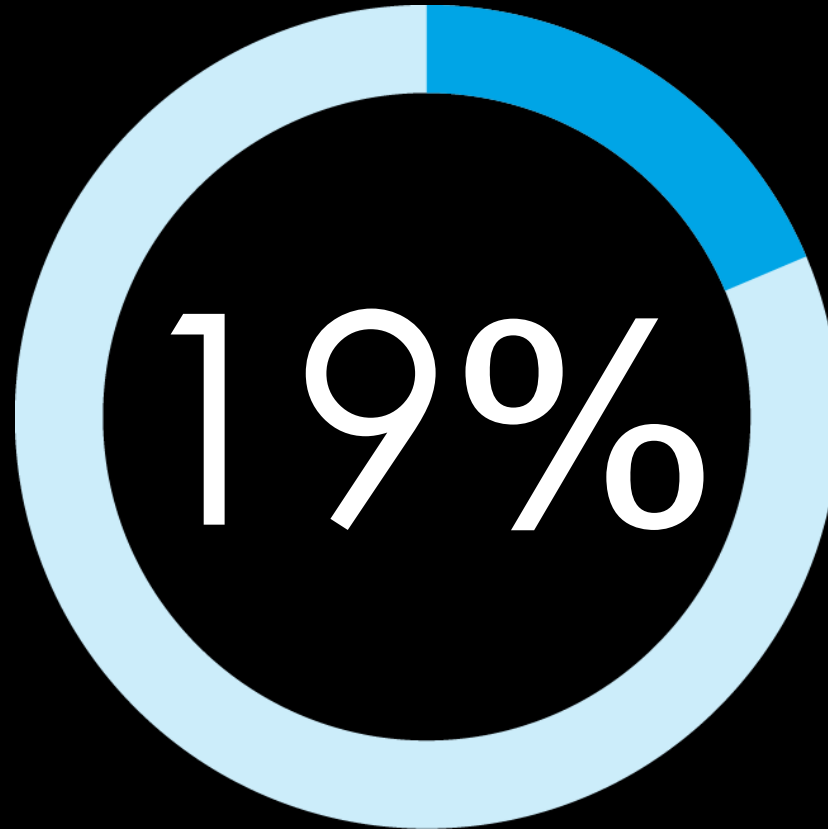
usernames, passwords,
phone numbers, and
physical addresses were
compromised from **eBay**.





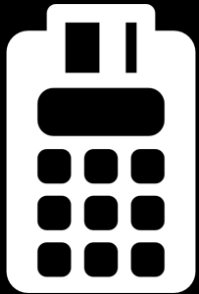
The average cost of each data breach is an estimated:

US\$ 3.62 million

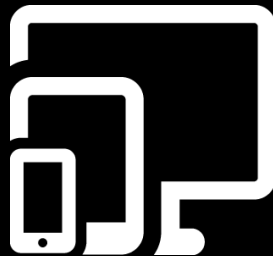


of consumers say they will cease shopping at a retailer that was breached, even if the problem was addressed and remedied.

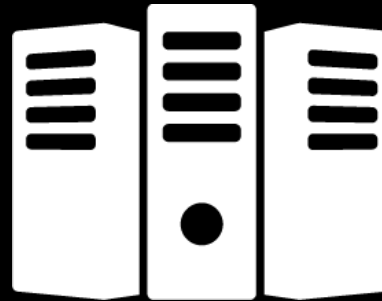
**In the Retail Industry, security vulnerabilities
can appear in any of the following
card-processing environments:**



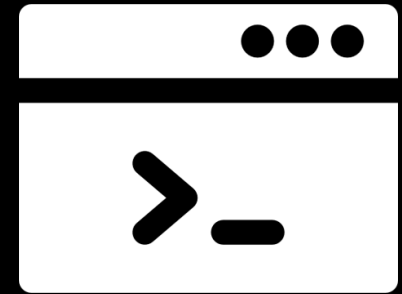
Point-of-sale devices



Mobile devices and PCs



Servers



E-commerce sites

To ensure all these environments have a set
standard of security protocols in place, is why
PCI-DSS was created.

PCI-DSS

Overview and Compliance

Payment Card Industry Security Standards Council (PCI-SSC)

In 2004, the PCI-SSC, made up of five major credit card companies: American Express, Discover, JCB, Mastercard, and Visa; established a set of security standards applicable to all members, merchants and service providers, that store, process, or transmit, cardholder data.

This security standard became the Payment Card Industry Data Security Standard: PCI-DSS.

**The latest standard:
PCI-DSS (v3.2),
was released in
April 2016.**

**This comprises of:
12 Requirements with
6 Control Objectives**

1. Build and Maintain a Secure Network and System
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

Build and Maintain a Secure Network and System

Requirement 1:

**Install and maintain a firewall,
configured to protect cardholder data**

The Firewall prevents unauthorized users from accessing your network and servers, which may contain cardholder data. To ensure that you are protected:

- Restrict all traffic from untrusted networks
- Ensure all traffic passes through the firewall
- Except for necessary protocols, deny all other traffic from the cardholder data environment
- Install firewall software, or equivalent, on all web-facing devices

Build and Maintain a Secure Network and System

Requirement 2:

Do not use vendor-supplied defaults for system passwords and other security parameters

By having an 'easy' password, hackers and cyber criminals can easily gain access to your network.

The Top 10 common passwords:

- | | |
|-------------|--------------|
| 1. 123456 | 6. 123456789 |
| 2. Password | 7. letmein |
| 3. 12345678 | 8. 1234567 |
| 4. qwerty | 9. football |
| 5. 12345 | 10. iloveyou |

Protect Cardholder Data

Requirement 3:

Protect stored cardholder data

Cardholder data should not be stored unless absolutely necessary. If you do, ensure the following precautions:

- Limit the amount of data stored, and retention time, to what is actually required
- Do not store sensitive authentication data after authorization, such as: cardholder's name, Primary Account Number (PAN), expiration date, service code, etc
- Mask PAN when displayed
- Ensure all security policies for protecting stored cardholder data are documented and implemented

Protect Cardholder Data

Requirement 4:

Encrypt transmission of cardholder data across open, public networks

Using exploits and vulnerabilities, hackers and cyber criminals can intercept transmission of cardholder data, over the open/public Internet. Using cryptography and security protocols, such as SSL/TLS encryption technology, can prevent hackers from successfully stealing such data.

Maintain a Vulnerability Management Program

Requirement 5:

Protect all systems against malware,
and regularly update anti-virus
software and programs

Malware (malicious software) includes: computer viruses, worms, trojans and spyware. These can be used to steal, encrypt, or delete cardholder data.

Today, there are over **1.5 million** zero-day malware, on the Internet. Thus, it is essential to stay up-to-date with the latest anti-malware updates and patches.

Maintain a Vulnerability Management Program

Requirement 6:

Develop and maintain secure systems and applications

By exploiting a security vulnerability in your network, hackers and cyber criminals can gain access to your network, and steal cardholder data. These vulnerabilities can be mitigated by regularly checking and installing the latest security patches.

If the process is fully automated, using PUSH technology, as the patches become available, the risk to your network will be greatly reduced.

Implement Strong Access Control Measures

Requirement 7:

**Restrict access to cardholder data;
genuine 'need-to-know'**

Access control allows you to permit, or deny, staff access to cardholder data. By restricting the access based on a need-to-know and job responsibilities basis, and granting the least amount of data and privileges needed to perform a job, cardholder data can only be accessed by authorized personnel.

Implement Strong Access Control Measures

Requirement 8:

Identify and authenticate access to system components

It is best practice to assign unique User IDs for all authorized personnel, who will have access to critical data and systems. That way, all actions performed on the system components, can be traced back to a User ID.

In addition, multi-factor authentication is required, for login.

Implement Strong Access Control Measures

Requirement 9:

Restrict physical access to cardholder data

With the rise in low-level social engineering methods, used by hackers and cyber criminals; part-time staff, contractors, consultants, and other onsite visitors, should be given very restricted physical access to cardholder data.

Use of temporary access cards, and denial of entry to restricted areas, is required.

Regularly Monitor and Test Networks

Requirement 10:

Track and monitor all access to network resources and cardholder data

If something does go wrong; logs, and user activity history, are essential for digital forensics. Implementing the following will help with this:

- Use audit trails, linking all access to system components, to each individual user
- Use audit trail entries for all system components for each event
- Secure audit trails so they cannot be altered
- Review logs, and security events, to identify anomalies or suspicious activity

Regularly Monitor and Test Networks

Requirement 11:

Regularly test security systems and processes

New vulnerabilities are constantly being exploited by hackers and cyber criminals. Thus, your systems should be tested frequently to ensure security is maintained over time:

- Implement processes to test for the presence of wireless access points
- Run internal and external network vulnerability scans, after any significant changes to your network
- Use network intrusion detection and/or intrusion prevention techniques, to detect and/or prevent intrusions into the network

Maintain an Information Security Policy

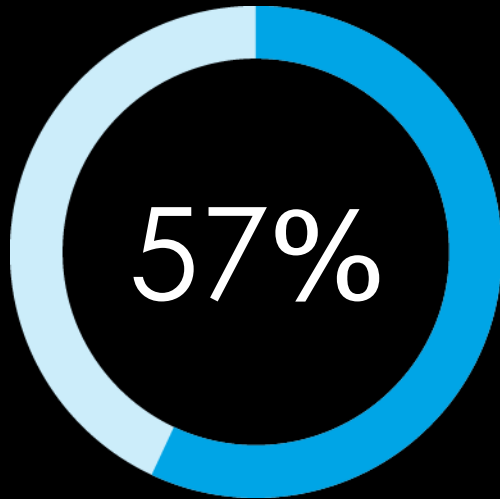
Requirement 12:

**Maintain a policy that addresses
information security for all personnel**

A clear and precise security policy is essential for all staff to be aware of the sensitivity of cardholder data, and their responsibility for protecting it.

- Establish, publish, maintain, and disseminate a security policy
- Review the security policy
- Implement a risk assessment process that is performed annually
- Ensure that the security policy and procedures clearly define responsibilities for all personnel

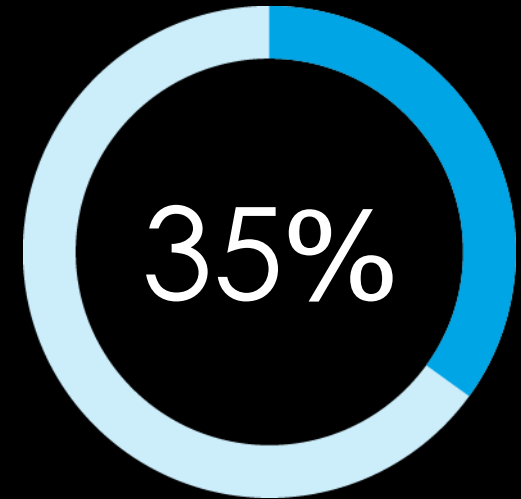
PCI-DSS Statistics



of businesses with one to six million transactions are still not PCI-DSS compliant

US
\$25,000

is the fine for businesses that are not PCI-DSS compliant



of businesses with more than six million transactions are still not PCI-DSS compliant

Seek professional help for your PCI-DSS Compliance

Staying PCI-DSS compliant, can take up valuable time and resources. By outsourcing your cyber security to a Managed Security Service Provider (MSSP), they can help gain and maintain PCI-DSS compliance.

In addition to PCI-DSS compliance, the benefits of using as MSSP includes:

- Safely/securely connecting multiple stores, branches, warehouses, remote sites
- Reduce operational costs by centralizing security policy management
- Reducing admin/operational overhead
- Protecting sensitive/confidential data and ensuring compliance with PCI standards
- Growing your network without sacrificing centralized control

Award-Winning Technology

FASTEST, Most Extensive, Cost Effective and Assured Protection

The logo for PUSH Technology, featuring the word "PUSH" in a bold, white, sans-serif font. The letters "P" and "S" are stylized with grey arrows pointing outwards from the center.

PUSH TECHNOLOGY
WHY WAIT?

PUSH Technology proactively pushes out and installs updates in an average time of less than **45 seconds**.

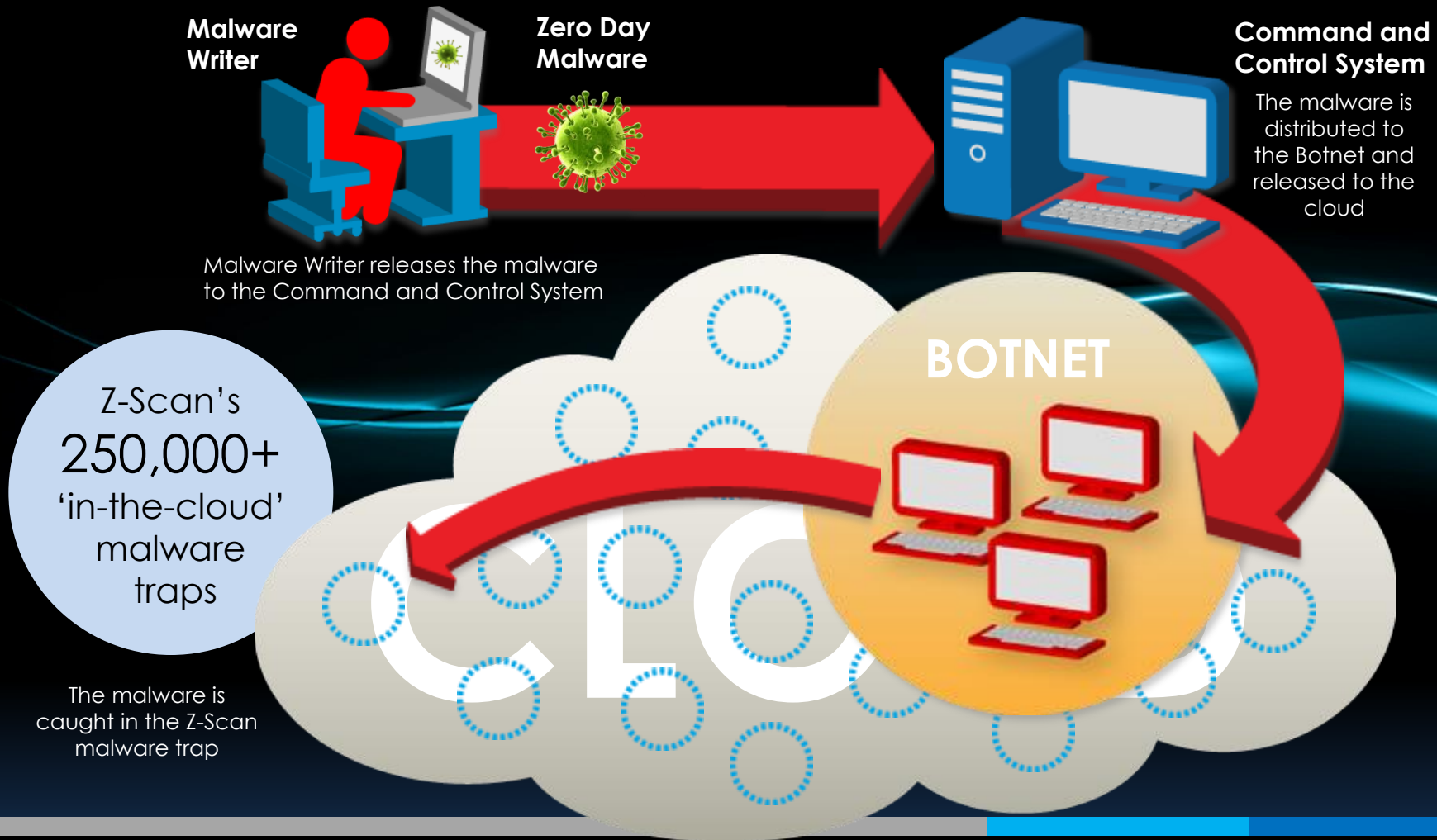
The logo for Z-Scan, featuring the word "Z-SCAN" in a bold, white, sans-serif font. The letter "Z" is stylized with a blue horizontal bar passing through it.

Z-Scan focuses on developing and releasing updates to protect against emerging zero-day malware with a best response time of **3 seconds** from a threat being detected.

In 2017, Network Box was PUSHing an average of **30,000** updates a day.

Z-Scan

Malware Detection



Z-Scan

Identification and Signature Creation

While the M-Scan Lab is doing analysis, Network Box Security Response utilizes the Z-Scan Outbreak system to protect Network Box clients around the world

**Z-Scan
Outbreak System**

Z-Scan's
'in-the-cloud'
malware traps



**Network Box Security Response
'Outbreak System' | M-Scan Lab**

The Zero Day Malware is sent to Network Box Security Response, as well as the Network Box M-Scan Lab

Z-Scan

Signature Release and Application



Z-Scan Outbreak System

Signatures are released to the
Security Operations Centers (SOCs)

**Network Box
User** End user's Network Box
receives a potential threat



The whole process takes
3 seconds

Z-Scan
immediately
replies with a
confidence level

**Z-Scan
USA Region**



**Z-Scan
Europe Region**



**Z-Scan
Asia Region**



The device
sends the
object hash
to the Z-Scan
cloud



PCI-DSS (v3.1) and (v3.2) Compliant

While Network Box does not directly store or process credit card information, a large number of our customers do, which brings them under the PCI Security Standard. Network Box, as service provider, can help you with gaining and maintaining PCI-DSS compliance.

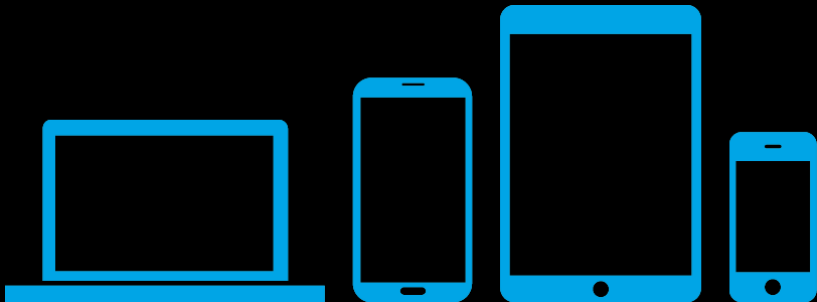
Other Security Threats

Top 5 cyber risks affecting most businesses and organizations today

5

Internet of Things (IoT)

The vulnerability of everything



Without proper protection, these Internet-connected devices are all vulnerable to cyber attacks and open to hackers.



1 million new devices connect to the Internet every 3 hours.



All scanned information on hard discs of MFCs (Multi-Function Centers) can be stolen.



Cameras used by most offices, industrial plants, hospitals, prisons, banks & the military can all be hacked.



Competitors & government agencies can listen to your VoIP (Voice over Internet Protocol) telecons.

4 DDoS

Distributed Denial of Service



DDoS attacks are up 149% compared to the same period the previously.

602 Gbps

Hacker group *New World Hacking*, launched probably one of the largest DDoS attack in history, reaching 602 Gbps.



Leveraging IoTs, an attack by the *Mirai BOTNET*, disrupted a large number of famous websites:

The New York Times, Netflix, Twitter, Google, VISA, CNN, Wall Street Journal, and PayPal.

3 Ransomware

Your computer files could be held for ransom



Ransomware is on the rise and many businesses and organizations have had to pay huge sums to free their files.



More than 300,000 computer systems in over 150 countries were affected by the recent WannaCry ransomware.



The global ransomware damage cost in 2017 is estimated to be in excess of US\$ 5 billion.

2 Internal Staff

They can be your biggest security risk



of users have the same password over multiple social media sites. By stealing and using passwords obtained from these sites, hackers could gain access to your network.



Your network could be in danger if you are using default passwords. By using the user name: *admin*, and password: *12345678*, hackers can easily infiltrate most networks and smart devices.



Social Engineering and other low tech methods can also be used to obtain your personal and confidential information, as well as access to your network



1

Procrastination

Don't wait to be a victim

If you do not have proper cyber security in place you could be vulnerable right now:



Hackers are probing your network every 2.3 seconds



A new virus is released every 12 minutes




66.5% of your email is Spam, Social Engineering, or Malware



The Bottom Line...

Businesses and organizations operate at the speed of **red tape**,
while hackers operate at the speed of the **Internet**.



**Who do
you think
is going
to win?**

**You cannot
escape the
responsibility of
tomorrow
by evading it
today.**

— Abraham Lincoln





NEXT
GENERATION
MANAGED SECURITY

Thank You

Jan van Leersum
Network Box Singapore
Managing Director

