huonit
A KYOCERA GROUP COMPANY

IT SECURITY PORTFOLIO

Protecting Australian businesses against a growing threat landscape.

Businesses, large and small, are frequently exposed to sophisticated cyber attacks across the globe. Cybersecurity is no longer the sole responsibility of your IT department. It's everyone's business.

Cyber attacks can take many forms including convincing email scams, ransomware attacks, CEO fraud, high profile website hacks, and more.

The worst part?

A single successful attack could seriously damage your business and cause financial burden for you and your customers, as well as affect your business's reputation.

IT SECURITY ISN'T A 'SET & FORGET' JOB.

The world of cyber-crime is always evolving. Criminals keep getting smarter, and so must businesses. An attack can come from a variety of sources. That's why it's important to educate your staff how to recognise cyber threats plus also reviewing your cybersecurity plans and processes.

This continuous process requires time, energy and resources. That's why you need a trusted partner that stays up-to-date with cutting edge IT security on your behalf, so you can focus on your core business knowing it's in safe hands.

At Huon IT we offer a range of IT Security Solutions including:

- **Strategic Services** - Cybersecurity Maturity Program
- **Proactive Monitoring** – Cyber Patrol
- **Audit Services** – Penetration Testing & Vulnerability Assessments
- **Defensive Systems** – Managed Infrastructure, Endpoint Antivirus, Email Filtering & Protection
- **Staff Education** – Cybersecurity Awareness Training

Strategic Services for Executive Teams

Huon IT's Cybersecurity Maturity Program is a 12-month long program for CEOs, Directors, CFOs, COOs, as well as IT & Compliance teams.

The purpose of the program is to guide leadership teams through assessment, planning and continued review of your organisation's cybersecurity strategy. This program is tailored to each business' unique requirements and the engagement typically follows three phases over a 12-month period:

This holistic approach enables businesses to set a baseline and:

- Identify – assets, policy, industry threats, and risk assessment.
- Protect – access controls, staff awareness and training, information protection policy, data security
- Detect – detection processes, monitoring
- Respond – response planning
- Recover – recovery planning

Audit Services

Security risks can lurk internally and externally. The following security audits should be conducted once every 1-2 years at a minimum (or more depending on your business' risk profile):

Network penetration testing (an external security check):

Cyber-criminals look for holes in your system – so we want to find them before they do. With a penetration test, you can safely see just how far a real-world attacker can actually get with your current IT security systems & address any holes before it's too late. This service tests any web-exposed elements of your network including:

- IP addresses,
- Websites, and
- Infrastructure

You will be provided with recommendations on how to fix these issues. If you need help to implement the changes, Huon IT's security experts are on-hand to help your team.

Vulnerability assessment (an internal security check):

While penetration testing is an external security check of your web elements, vulnerability assessments identify wider risks within your network setup. They include a review of your:

- Core infrastructure (including switches, routers, firewalls, applications etc.) and
- End-user security (e.g. anti-virus, anti-malware, mobile devices and password policies).

Proactive Monitoring

To defend Australian business networks and devices against malicious threats, abnormal user behaviour and data breaches, Huon IT's Security Operations Centre (SOC) operates 24/7, 365 days a year.

In the Cyber Patrol service you will receive:

- Daily 24x7 monitoring via our world class Security Incident & Event Management (SIEM) system.
- Weekly vulnerability scans & reports to identify any new potential weaknesses.
- Expert analysis by real people reviewing and validating issues, around the clock.
- License per device for an affordable monthly fee.

Defensive Systems

There are several layers to defensive IT security that you need to address, and each is as equally important to ensure your business is safe. These include:

- Managed infrastructure
- End-point antivirus
- Email patrol

Managed infrastructure FORTINET paloalto hp CISCO

Firewalls, switches, routers and access points are all key elements of your network that need to be managed to ensure optimal performance and security. Huon IT can provide hosted hardware for a simple PAYG monthly fee, or provide managed services for your existing BYO devices.

End-point antivirus WEBROOT SOPHOS

Every time your employees access the internet on a device holding company data, they expose your business to risk. Huon IT will design and implement an end point security solution with antivirus and malware protection for desktops, laptops, virtual machines, tablets and smartphones.

Email filtering & protection mimecast

Email is the source of many IT security risks. With scam emails becoming more and more convincing, staff education and vigilance can only go so far. Huon IT's cloud based email filtering and spam scanning service will stop suspicious emails before they reach your network.

Staff Education

Even with the latest and greatest technology safeguards in place, the "human factor" can still leave you exposed to risk.

To minimise the risk of users inadvertently clicking on suspect links, accidentally releasing their password or unintentionally downloading malware, education is more crucial than ever before.

mimecast KnowBe4 Human error. Conquered.

Huon IT's Cybersecurity Awareness Training is conducted over a 12-month period. It covers:

- Baseline testing
- Training your users
- Regularly phishing your users
- Reporting and re-training as required.

THE IT SECURITY FAST FACTS:
HOW DO YOU STACK UP?

CYBERSECURITY THREATS ARE ON THE RISE

A new report from Juniper Research in 2019 found that the cost of data breaches will rise from $3 trillion each year to over $5 trillion in 2024.

ON AVERAGE, BUSINESSES TAKE OVER SIX MONTHS TO IDENTIFY A DATA BREACH

The average time to identify a breach in 2019 was 206 days, and the average time to contain a breach was 73 days.

Source: Ponemon Institute 2019

EMAIL FILTERS CAN FAIL

In December 2018, Mimecast claimed that 12% of spam, phishing and malware emails were making it through to inboxes.

AUSTRALIAN CEOs ARE CONCERNED

Eighty-five percent of Australian CEOs pointed to cyber security as a greater threat to growth than any other concerns.

Source: PWC CEO Survey 2020

PHISHING ATTACKS CONTINUE TO BE ONE OF THE MOST POPULAR WAYS TO ATTACK BOTH BUSINESSES & CONSUMERS

The number of phishing sites detected grew 220% between January and December 2018 (up 36% from the previous year).

Source: 2019 Webroot Threat Report

URL OBFUSCATION IS FREQUENTLY USED TO DIRECT USERS TO A MALICIOUS SITE

A massive 40% of malicious URLs were found on good domains, since legitimate websites are frequently compromised to host malicious content.

Source: 2019 Webroot Threat Report

ONE OF THE GREATEST RISKS TO IT SECURITY INTERNALLY IS HUMAN ERROR

Respondents in Telstra's Security Report 2019 indicated that 25% of security breaches internally will come from accidental insiders, 11% from targeted insiders and 8% from malicious insiders.

To prepare for the worst, only trust the best. Contact the security experts at Huon IT today for custom advice on how to ensure your business is safe.

huonit
A KYOCERA GROUP COMPANY

www.huonit.com.au | info@huonit.com.au | 1300 HUON IT