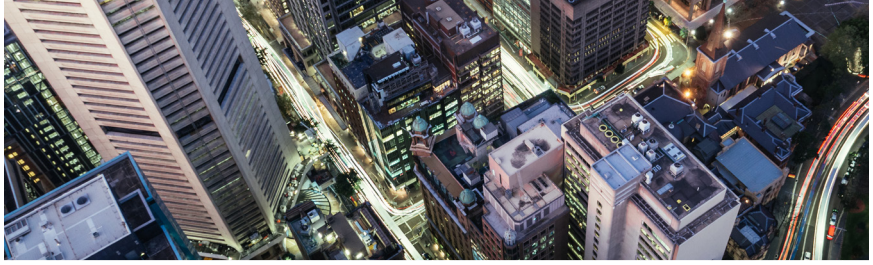
RMS READY TO HELP



RMS INSIGHT July 2017

CYBER CONFIDENCE: The Human Firewall

The risks we face are potentially higher than secular organisations, which are not focused on making disciples.

Christian organisations such as ours pride themselves on their purpose, centred around leading people to Christ. A significant emphasis is placed on living a Christ-centred life, upholding attributes such as trust, friendliness and helpfulness. It is through our personal interactions with people that we hope to share His love with those around us. What happens, however, when people take advantage of our generous and trusting spirit? Without losing sight of these qualities, how do we strike a balance that ensures we protect our sensitive information and systems?

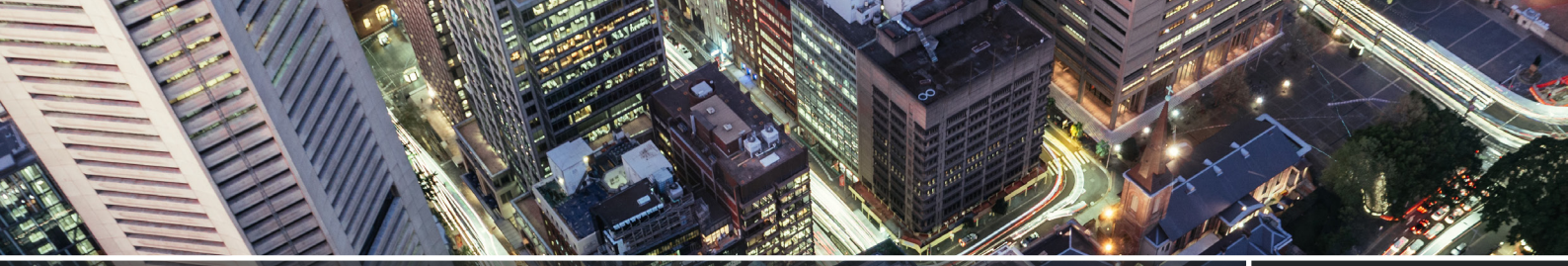
With physical interactions, it tends to be easier to recognise something odd about a person or suspicious activities by analysing people's body language, tone, eyes and gestures. We have physical security like doors and locks to help guard against unauthorised access. With interactions through technology, however, we have far fewer clues about a person we are communicating with, so we often give them the benefit of the doubt rather than risk offending them. The risks we face are potentially higher than secular organisations, which are not focused on making disciples.

A recent study, Managing Insider Risk Through Training & Culture (2016), asked more than 600 people at companies currently running security and privacy training programs about their information security experience. The study found that more than half (55 per cent) had already experienced a security incident due to a malicious or negligent employee. "Among the many security issues facing companies today, the study emphasises that the risk of a data breach caused by a simple employee mistake or act of negligence is driving many breaches. Unfortunately, companies continue to experience the consequences of employees either falling victim to cyber-attacks or exposing information inadvertently," said Michael Bruemmer, vice president, Experian Data Breach Resolution.

With privacy legislation now a significant compliance requirement and new mandatory disclosure of breaches now in effect — along with the relentless global ransomware and malware attacks — the stakes are higher than ever. No longer are the risks limited to one person or even one office. The risks can extend to the entire organisation as we all share the same brand and identity.

by Matthew Mulligan
Adventist Church Technology Services

SEVENTH-DAY ADVENTIST CHURCH South Pacific



RISK MITIGATION

There are several steps that companies can take to better equip their employees with the skills required to help protect company data. This however requires a move beyond standard employee training and a shift to a security culture.

For years now we have all spent considerable time and effort implementing technical filters or firewalls to block threats. However today it is simply not enough.

You might think that your spam filter will catch any malware and if not, your local anti-virus will. Think again. Approximately one in 200 emails with malicious content makes it through. This means that there is the potential for malware to make it through to your inbox every day. So we also need a highly effective "human firewall".

Employees are the last line of defence and need to become a dynamic security layer to help guard against attacks that make it through all your technical filters. This will challenge us to our core as it requires us to apply filters that question our value and trust.

Cyber threats today are real and they are constant and growing in their scope and complexity. So our defences must grow to ensure we remain on guard.

So what can we do to ensure our human firewall is effective?

- Only interact with documents, links and attachments from people you know and with communications you are expecting.
- Treat unsubscribe buttons with caution. It's best to simply delete unwanted emails as unsubscribe links can themselves be loaded with malware.
- Provide regular training for your staff using current examples.
- Randomly test your human firewall with spot checks to see where it can be improved.
- Ensure staff really understand the full picture so they know why they need to take these extra precautions.
- Have users only access data that they genuinely need access to for their job and ensure they know how to handle the data safely.
- Classify your data so you know what is sensitive and put in place extra controls to protect it.
- Encrypt sensitive data.
- Ensure you backup your data regularly and store it offline and unplugged from power.
- Your users need to be trained so that when they pick up the phone they understand that the person on the other end might be a criminal hacker who tries to manipulate them into getting access to the network. The person may impersonate "Tech Support" and ask for a password, or pretend to solve technical problems and compromise the workstation. They may also just be looking for details to help them sound more credible for another call.
- There are now thousands of devices like watches, fridges and TVs all connected to the internet. Your employees need to be trained to change the default passwords and disable remote access.
- Employees need to be enlightened about the dangers of shadow-IT and understand the risks of signing up to a range of free online services bypassing the traditional IT solutions.
- Mobile apps are increasingly vulnerable to and used for attacks. Ensure your staff only install apps that they specifically need from reputable vendors and refrain from installing apps for entertainment and unknown vendors even if it is through the official App Store.

NOW IS THE TIME TO TAKE CYBER SECURITY SERIOUSLY.

"Your human firewall encompasses how well employees understand the importance of the right security practices and how easily they can act on them."

Right now, most organisations aren't doing an adequate job, but there are steps that companies can take. It starts with focusing on both technology and the people using it. However, these protocols should also resonate with employees.

Creative communication techniques — such as webcasts and quizzes — can help employees realise the importance of security practices by linking important aspects of security from their private lives to their work lives. Engaging employees will also help security teams overcome the challenge of employees viewing security as an obstacle that prevents them from doing their work. Instead, when security becomes personal, employees are encouraged to be active partners in helping to protect the organisation.

Company leadership in partnership with security teams should reward employees who embrace security practices and discourage behaviours that threaten security.

Ultimately, an email security program is only as secure as the people using it, but your employees can't do it alone.

Working together to create a culture of cyber security is the way forward in strengthening our human firewall.

THE CYBER SECURITY CULTURE

1. **Comprehensive security protocols are in place** and working partnerships are built within the business.

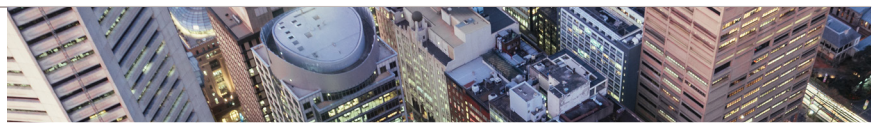
2. **Employees are educated and engaged** on how to use security tools properly and are aware of their individual responsibilities and, with ongoing training and communications, have a good understanding of company policies.

3. **Security best practices are implemented** - i.e., policies for acceptable use, information classification, access control, encryption, patching, vendor agreements, incident response, business continuity and compliance.

RMS READY TO HELP

with expert knowledge from

ADVENTIST CHURCH TECHNOLOGY SERVICES



RMS INSIGHT - ABOUT THIS RESOURCE

RMS INSIGHT is a project of Risk Management Service. It represents our collaboration with other services, ministries and departments of the Adventist Church. We work together to deliver relevant and timely business insight from the risk and safety space to Adventist Church professionals.

This Cyber Security resource was written by Matthew Mulligan (Adventist Church Technology Services) and prepared by RMS.

If you would like to collaborate on a risk or safety topic, talk to RMS.

SEVENTH-DAY ADVENTIST CHURCH South Pacific