Nine Steps to Smart Security for Small Businesses

by David Lacey
Co-Founder, Jericho Forum

Nine Steps to Smart Security for Small Businesses

TABLE OF CONTENTS

INTRODUCTION

If you're a small business, we salute you. Small enterprises are the engine of our economy, generating innovation, employment and wealth, so your security matters. This guide shows how you can reduce your risks at an affordable price.

Good security ensures business is carried out efficiently, correctly and without interruption.

Data breaches are bad for business, so every enterprise needs security. In the past this was expensive, because security products were designed for companies with deep pockets and teams of experts. But that's changed. New 'cloud based' services, such as those offered by Qualys, are fast to deploy, safe and easy to use. What's more they're even more affordable.

With growing demands from customers and regulators for security, now is a good time to invest in security. Leading cloud-based security services deliver a professional level of security assurance in a form that fits the circumstances and pockets of small businesses.

WHY SHOULD I BOTHER?

Your business depends on computers and data. They help you advertise products, capture orders, process payments and keep accounts. Good security ensures business is carried out efficiently, correctly and without interruption. It's a smart investment, helping you to:

- Avoid losses from theft (of data or equipment)
- Save time wasted dealing with security incidents
- Recover faster from equipment failures
- Retain customers and win new business
- Meet your legal and compliance obligations

Security is mandatory if you handle sensitive personal data or process payment cards. Customers expect it, and many supervisory bodies demand it, especially in financial services, healthcare and government sectors. A good reputation for security will help you win and retain business. It's an unwritten 'licence to operate' in markets that value security.

AREN'T FIREWALLS AND ANTI-VIRUS ENOUGH?

By applying a small number of smart, simple measures you can substantially reduce your security risks. Make sure, however, that you don't leave any big gaps in your defences. Firewalls and anti-virus protection are essential, but they are not enough. Today's attacks are designed to search out and exploit weaknesses in your system. It's vital, therefore, that you frequently scan your systems for vulnerabilities in your set up, and take appropriate action to fix them. Fortunately, this is not as difficult as it sounds with the help of a trusted, online scanning service.

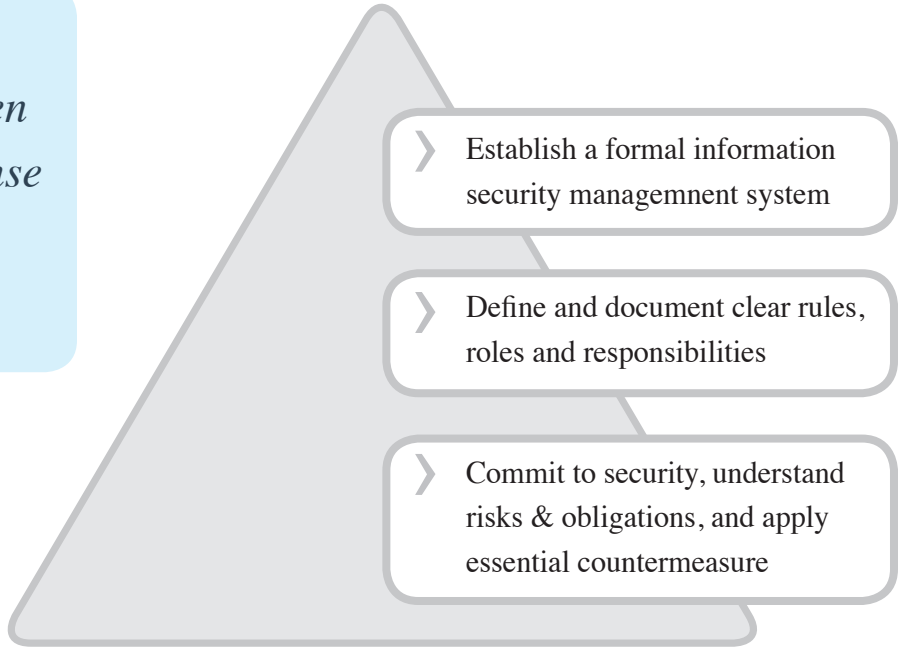
The global reach of networks and the growth in underground software skills increase the scale and sophistication of criminal security threats. Enterprises today face 'zero day' and 'minus day' attacks designed with unprecedented levels of planning, skills and determination. But worse is to come. Most breaches result in short term impacts, such as a temporary outage or a limited compromise of data. Few have long term consequences, such as irrecoverable damage to an essential database. Such threats will inevitably emerge as terrorist groups and other 'bad actors' become aware of the potential for such attacks and acquire offensive capabilities. Future risks are likely to be more serious than anything previously experienced.

A good reputation for security helps you win and retain business.

In addition to technical measures, you need safeguards against physical security breaches, whether deliberate or accidental. But keep it simple. Don't attempt to implement big company standards such ISO/IEC 27001, unless you're experienced. They might help you win work from big organisations, but they involve a lot of paper, and require prior knowledge of professional security practices.

If you're a medium sized business or have aspirations to grow, you'll also have to define responsibilities, set standards and check things get done. The need for policies, procedures and audits grows with the size of the organisation. But aim to strike the right balance between applying common sense and following procedures. A tiered approach to security is recommended. Start with a minimal set of measures and then add layers of further control to build a more effective management system.

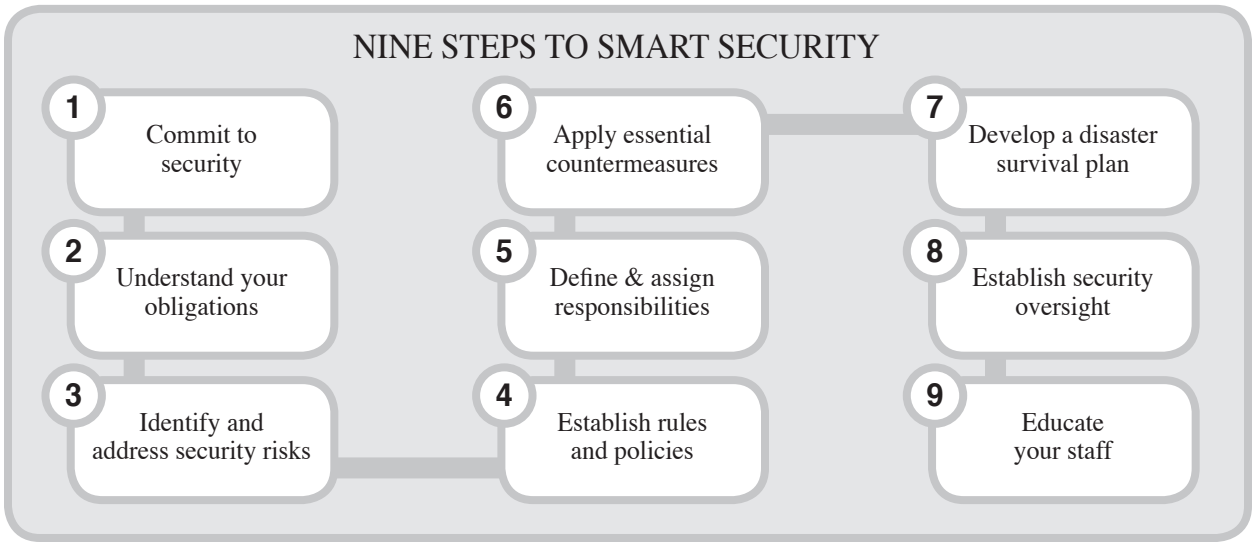
Aim to strike the right balance between applying common sense and following procedures.



Levels of sophistication - Start at the base and work upwards

NINE STEPS TO SMART SECURITY

Here are nine steps, in order of priority, for implementing security in a small or medium sized business.



STEP 1:
COMMIT TO SECURITY

A simple but powerful first step is to set out your commitment to information security in a written declaration. This shows you're serious and communicates the fact to staff and stakeholders. It can take the form of a formal security policy, or a simple, signed statement, stating that your enterprise aims to apply its best endeavours to safeguard sensitive data and protect critical business systems from security risks.

A written undertaking shows you're serious, and communicates this to staff and stakeholders.

STEP 2:
UNDERSTAND YOUR OBLIGATIONS

Next, ensure that employees who handle sensitive information or control critical systems are aware of legal, regulatory or commercial requirements for security, including the consequences of failing to meet them. One example is data protection and privacy legislation, which requires everyone handling sensitive, personal data to safeguard it according to strict principles. A further example is the Payment Card Industry Data Security Standard (PCI DSS) which requires retailers who process payment cards to:

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

STEP 3:
IDENTIFY AND ADDRESS SECURITY RISKS

To select the most appropriate measures for your money, you need to understand the security risks to your business assets or activities. Consider your exposure to security threats, such as:

- Theft of data or equipment
- Espionage
- Fire or floods
- Equipment failures
- Computer viruses and 'malware'
- Computer hacking

Assess how vulnerable your systems, equipment and premises might be to these threats, and identify the best means of reducing the risk.

Qualys provides a range of easy-to-implement, automated PCI compliance solutions for merchants and acquiring institutions.

These products are also widely used by big companies to test the security of their contractors.

You can also have a free 14-day trial of the services with 24x7 support to help you identify.

And there's no need to install any software since they use an innovative, 'Software as a Service' (SaaS) approach.

Caution: You can buy many specialist products to scan your computer servers for known exposures. But it's vital to ensure they're genuine. Some advertised products are dangerous sources of malware infection. With Qualys services, you can rest assured that your systems are safe.

STEP 4:
ESTABLISH RULES AND POLICIES

Draw up a list of "Do's and Don'ts" to ensure your employees follow the essential rules needed to safeguard sensitive data and critical business services. Ensure these rules are regularly reviewed and updated. Examples might include:

DO	DON'T
• choose strong passwords and change them regularly	• share customer data with outside parties
• lock away laptops and sensitive data when the office is vacated	• leave mobile devices unattended in public places
• take regular back-up copies of your data	
• apply critical security updates and anti-virus updates promptly	

In a larger business, a written policy, setting out principles and objectives in a more structured manner is a better source of guidance for managers and staff. Procedures for key security processes, such as controlling access rights, issuing equipment and taking back-up copies, should also be defined, along with responsibilities for keeping them current.

STEP 5:
DEFINE AND ASSIGN RESPONSIBILITIES

Assign roles and responsibilities for safeguarding key assets (such as premises, equipment and data) and carrying out security activities (such as taking back-ups or managing access rights). Deputies should be assigned for essential tasks, to ensure they are carried out during leave and absences.

STEP 6:
APPLY ESSENTIAL COUNTERMEASURE

Ensure there are measures in place to protect equipment and data from theft, damage and unauthorised access. They should include the following.

- Physical measures for premises, such as access control, intruder alarms and lockable cabinets for sensitive or valuable assets.
- Procedural controls, such as choosing passwords, taking back-ups and locking away papers and laptops when offices are vacated.
- Technical measures such as firewalls, anti-virus software and back-up devices. It's vital also to ensure critical security updates are promptly applied.

Ensure products are genuine, as some are a dangerous source of malware infection.

Security technology can be used to safeguard sensitive data and prevent or detect potential incidents. Examples of security products that are becoming increasingly essential for everyday business use include:

- Strong authentication devices for remote access by home or mobile users
- Hard disk encryption systems to protect data on laptops
- Intrusion prevention systems to block incoming attacks from the Internet
- Vulnerability management technologies to monitor the exposure of networked computers to potential attack

Caution: Professional advice can help you select the right products and install then correctly. Be careful, however, to use only services from an established brand or those recommended by a knowledgeable and trusted source.

STEP 7:
DEVELOP A DISASTER SURVIVAL PLAN

Prepare your enterprise for hazards such fire, flooding or equipment failures. Advance thinking and preparation will reduce the damage to business operations and speed up recovery from failures.

Advance thinking and preparation will reduce the damage to business operations and speed up recovery from failures.

- Identify alternative working arrangements, such as fallback sites and systems
- Draw up a simple plan and keep up-to-date back-ups of essential data and software at a secure, remote location
- Nominate a crisis team to enable a fast response without duplication of effort
- Assign responsibilities for dealing with emergency services, contacting customers and getting fallback systems up and running.

STEP 8:
ESTABLISH SECURITY OVERSIGHT

In busy working environments, security tasks can be overlooked. Implement checks to prevent this happening. Larger businesses might consider a more formal form of governance, with objectives, performance measures and audits.

STEP 9:
EDUCATE YOUR STAFF

All employees should be educated in basic security practices, and regularly reminded of relevant security risks, as well as their own responsibilities. Begin with induction sessions for new staff and maintain awareness through regular briefings or bulletins.

Security is everyone's responsibility within a modern enterprise, so all employees need to be educated.

A range of educational material is available on the Internet. It costs nothing to point your staff in the right direction. Take a look at Get Safe Online (www.getsafeonline.org) for a good source of free advice.

CONCLUSION

Security has never been more in demand, and with today's Internet based cloud services, you can easily and cheaply implement professional monitoring services to measure your exposure and demonstrate your compliance. Now is the time to act. Start with simple, practical measures and build upon your experience. Qualys can't make you an instant security expert but Qualys services can deliver a level of professional support that has previously required a team of on-site experts.

HOW QUALYS CAN HELP

Qualys is the leading provider of on-demand security risk and compliance management solutions, enabling you to easily and cost-effectively ensure that your systems are secure and compliant. Using an innovative, Software as a Service (SaaS) approach, Qualys' solutions can be deployed within hours anywhere in the world.

QualysGuard® delivers continuous protection against the latest security threats without the substantial cost, resource and deployment issues associated with traditional software. It allows you to quickly and accurately scan your server for vulnerabilities that could be exploited by an attacker. If vulnerabilities exist, it will find them and provide you with detailed information about each risk and links you to advice on how to mitigate these risks.

QUALYS IT SECURITY & COMPLIANCE SUITE FOR SMBS

Everything a business needs to identify risks and ensure compliance. QualysGuard® automates the process, providing network discovery and mapping, asset prioritization, vulnerability assessment reporting, and remediation tracking according to your business risk. Policy compliance features enable businesses to audit, enforce, and document compliance with internal security policies and external regulations.
QualysGuard® Security and Compliance Suite for SMBs includes:

- **QualysGuard Vulnerability Management**
  Quickly Deployable, Scalable Security Risk and Vulnerability Management
- **QualysGuard Policy Compliance**
  Define, Audit, & Document IT Security Compliance for your Business
- **QualysGuard PCI Compliance**
  Automated PCI Compliance Validation for Merchants and Acquiring Institutions
- **QualysGuard Web Application Scanning**
  Automated Web Application Security Assessment and Reporting
- **Qualys SECURE Seal**
  Web Site Security Testing Service and Security Seal that Scans for Vulnerabilities, Malware, and SSL Certificate Validation

QualysGuard® is used by more than 5,000 organizations in 85 countries worldwide, including leading organizations, as well as small and medium sized business in consulting, financial, government, healthcare, insurance, manufacturing, retail and technology.

For more information visit: http://www.qualys.com/

ABOUT THE AUTHOR

David Lacey is a well known information security expert, with more than 25 years experience in directing security programmes for organisations, including Shell and Royal Mail. He is now a researcher and writer, and author of the books “Managing the Human Factor in Information Security” and “Managing Security in Outsourced and Off-shored Environments”.