SMART DOLPHINS IT SECURITY SELF-ASSESSMENT TOOL

Proactive IT - Smart Security

No matter the size of your business, network security is now a requirement for every organization. We've developed this self-assessment tool to help you identify potential vulnerabilities. You'll find out how your organization fares when it comes to the overall state of your network security.

How it Works

It's pretty simple. The assessment begins on the next page and is a collection of categories related to your network security. Each category has a set of opposing statements that are intended to give you a frame of reference; each statement illustrates what each of the spectrum looks like within the category. Using these statements as guideposts, you will rank your own organization on a scale of 1 to 5 in each category.

For example, if you feel your business more closely matches the statement on the left, you will probably want to give your business a 1 or a 2. If you feel your reality is more like the statement on the right, then give yourself a 4 or 5. Obviously, you might give yourself a 3 if you are in the middle or undecided.

When you're done scoring all of the categories, add up your score across all categories. This total score will fall in one of the ranges described on the last page.

Success!

Success requires action. Review some of your lowest scores on this assessment and make an action plan for improvements. Focus on just one or two areas at a time and set a timeline for completion. Repeat.

If technology is important to your company you'll want to have a process of regularly reviewing your IT security in the various areas we review in this assessment. Over time, you should see a steady increase in your assessment score as well as a corresponding increase in the results you enjoy from your IT. We hope you'll find this tool a critical part of your success.

Connect with a Dolphin!

Feel free to call on Smart Dolphins. If you need help with this assessment or would like to have a complimentary network security audit, give us a call. Our Business Technology Navigators work hard with our clients to ensure they score well and we'll work with you too, to develop an IT roadmap that will reduce your organization's network risks.

YOUR ASSESSMENT

1 ⟵ 3 ⟵ 5

CATEGORIES	1 STATEMENT	5 STATEMENT	SCORE
Regular Network Security Audit	Network security audits only happen reactively and not regularly.	Audits are scheduled and led by a team or an outsourced IT service provider every six months.	
Anti-virus, Anti-spam, Firewall	We have anti-virus, anti-spam and a firewall in place but we are not certain these measures are up-to-date or effective.	Our business-grade firewall, anti-virus and anti-spam keep our IT protected. We've never had any security incidents to date.	
Monitoring and Tracking	Only incidents are tracked and we do not have any automatic monitoring tools.	We have automated monitoring in place, as well as device tracking software in case of theft.	
Patch Management	Some patches are done on an as needed basis.	All servers and workstations are kept up-to-date with the latest patches and up-dates are verified.	
Business Continuity	We have a backup but it is rarely tested and we are not certain we could recover from a malicious attack in a timely matter.	A robust data backup solution is in place which is tested regularly. Our disaster recovery plan is reviewed and kept up-to-date. Backups are isolated from possible ransomware infection points.	
Strong, Complex Passwords	We do not have a password policy.	Complex passwords are defined and enforced. All user passwords expire every 120 days or less.	
		SUBTOTAL FOR THIS PAGE:	

YOUR SCORE

CATEGORIES	1 STATEMENT	5 STATEMENT	SCORE
User Training	We do not offer our employees any security training.	Cyber security training and awareness is provided annually to new and existing employees.	
Network Security Budget	We have a limited IT budget and only a small percentage is allocated to network security.	Network security is our biggest IT expenditure.	
Physical Security Measures	Physical security measures include an office security system and a locked server room.	Access to our office and server room is restricted to authorized personnel, logged and reviewed. We have a security alarm, a nightly closing protocol, and our server room has additional security measures.	
Access Control Policy	We do not have any user control policies.	We have a clearly defined and enforced screen lock policy.	
Wi-Fi Use	Wi-fi is permitted without any restrictions.	Public wireless access is segregated from the private network.	
Third Party Software	Only some data in use by third party software is backed up.	All data in use by the third-party software is stored in a location that is backed up and tested.	
		SUBTOTAL FOR THIS PAGE:	
		SUBTOTAL FROM PREVIOUS PAGE:	
		TOTAL SCORE:	

NETWORK SECURITY ANALYSIS

Well Developed (65 or higher)

Your organization has worked hard to eliminate risk from your IT network. Staff are updated and tested on emerging threats and safe computing habits. Written security policy is in place and employees are aware of expectations and requirements around the use of the IT infrastructure. IT security and business continuity are central in your organization's annual plan and budget. Management is highly engaged in IT security. Continue to regularly perform security audits and make updates as needed.

Maturing (48-64)

You have made numerous improvements, not just technical but also to security policy and process. A substantial amount of your IT budget is invested specifically in security. Security and data handling policies are generally consistent. Ongoing network security education is not yet fully systematized resulting in a workplace IT environment where staff may not be fully engaged or understand their roles and responsibilities.

Inconsistent (36-47)

Your approach to network security is haphazard. While you may have added a few security improvements, your aging system has put your organization at risk. Security and risk awareness of staff varies throughout the organization. Password and network security policies are not fully enforced or standardized. Data security and access controls are not fully developed. Some unauthorized users can access sensitive data. Sensitive data storage is spread across network.

Fragile (24-35)

You may have experienced a few security incidents but the organization has managed to avoid a major disaster. Your network may be showing signs of poor performance. Aging infrastructure further contributes to security risk and lost productivity. The status of your backup and business continuity is unknown or inadequate. Security and risk awareness of staff varies greatly. Generally, there is a low level of safe computing knowledge throughout organization.

High Risk (below 24)

We recommend taking immediate action to implement standard network security tools, processes and policies. Your organization's network security is a ticking time-bomb and you'll need to seriously increase your technology investment to get your organization on track. Reach out to an IT service provider immediately.