IT SECURITY LEVELS

ALDRIDGE

START PROTECTING YOUR BUSINESS

Cybercrime is a legitimate threat, and your business is a potential target. Today's business leaders need to understand the threats facing their business and develop an appropriate security posture in response.

IT Security Posture – Your organization's approach towards IT security; your security tools, your culture, and your ability to react to continuously evolving threats.

UNDERSTAND YOUR RISK

You need a deep understanding of your IT security and how it fits into your overall risk management strategy. If you don't have a clear picture of your IT security, **don't just assume you have everything that you need**. Take the time to meet with your IT team and understand what they are doing to protect your business. If you are outsourcing IT, your provider should keep you informed on your IT security and risks in your regular IT strategy meetings.

ALDRIDGE'S IT SECURITY LEVELS

We developed our **IT Security Levels** to make IT Security more approachable. This outline breaks down IT Security into simple 'levels' comprised of technical security elements and behavioral factors. Try and determine your organization's security level. Are you where you need to be?

SECURITY LEVEL	TYPICAL BEHAVIORS	WHO SHOULD BE HERE?
-1 BLIND Security isn't just ignored; it is actively dismissed	› Believes they have nothing worth stealing › Uses corporate login credentials on random websites › Works from unmanaged personal devices	› Not recommended › Hobby or home-based businesses may be here
0 TOKEN Minimal effort to "be secure"	› Creates exceptions to security policies (i.e. turn off MFA for some people) › Lacks any security incident planning › Ignores security procedures for convenience	› Not recommended › Businesses with very small IT footprint (100% SaaS and only a few PCs) may be here
1 AWARE Importance of security is recognized	› Considers security component while thinking through business initiatives › Sacrifices some convenience for drastic improvements to security	› Values security but just beginning security journey › Lacks the budget for all desired security elements
2 ATTENTIVE There is an established top-down "security culture"	› Conducts security awareness training for entire team (i.e. how to spot a phishing attack) › Everyone, not just leadership, sees the importance of security	› Businesses who are willing to invest on their security journey › Able to achieve security commensurate with risks
3 VIGILANT Security is a priority, may have regulatory obligations	› Keeps up with current security trends or new threats › Conducts periodic security audits › Scans external environment for threats	› Has significant risks (highly valuable data) › Subject to regulatory requirements
4 RESILIENT Security is core to the overall business strategy	› Engages in digital forensics after attacks › Retains internal IT security experts › Applies mature risk management philosophy towards IT security	› Has significant risks and are common target for attacks › In the finance industry or regulated by SEC
5 INTEGRATED No compromises on security; desire to be on the cutting-edge	› Creates custom security policies and plans › Performs routine mock attacks on their environment to find weak points › Includes security role on leadership team	› Businesses that due to their risk or status require the highest level of security and assurance that it is providing the expected protection

IT SECURITY LEVELS

Security Tool/Service	Blind -1	Token 0	Aware 1	Attentive 2	Vigilant 3	Resilient 4	Integrated 5
Customized Policies and Procedures							✓
SOC & Security Information Event Management (SIEM)						✓	✓
Vulnerability Management						✓	✓
Dark Web Scanning					✓	✓	✓
Penetration Testing					✓	✓	✓
Vulnerability Scanning				✓	✓	✓	✓
Managed Detection & Response (MDR)				✓	✓	✓	✓
Security Awareness Training				✓	✓	✓	✓
Advanced Multi-Factor Authentication				✓	✓	✓	✓
Continuity Readiness				✓	✓	✓	✓
Endpoint Detection & Response (EDR)			✓	✓	✓	✓	✓
Advanced Email Filtering			✓	✓	✓	✓	✓
Basic Multi-Factor Authentication			✓	✓	✓	✓	✓
Managed NextGen Antivirus (NGAV)			✓	✓	✓	✓	✓
Basic Web Filtering			✓	✓	✓	✓	✓
Templated Policies and Procedures			✓	✓	✓	✓	✓
Backup and Recovery Readiness			✓	✓	✓	✓	✓
Basic Email Filtering		✓	✓	✓	✓	✓	✓
Managed Business-Class Firewall		✓	✓	✓	✓	✓	✓
Managed Legacy Antivirus		✓					
Unmanaged Legacy Antivirus	✓						
Consumer-Grade Router	✓						

AICPA SOC | MSP Verify™