ADVANCED LOGIC

BUILDING YOUR INFORMATION SECURITY PROGRAM IN 2024

A ROADMAP FOR BUSINESS CONTINUITY & SAFETY

Ransomware's effectiveness at disrupting businesses has exposed the lack of validated information security. Adopting a best-practices framework for Information Security helps organizations proactively prepare, minimize impact, and meet validation standards that are fast becoming the norm in all industries.

WHAT'S CHANGED?

Ransomware has proliferated in large part because organizations have become so reliant on digital; yet have not focused on safeguarding data as an operational priority. For too long, data protection and information security investments were made with the tacit assumption that things were being handled. Often by under-staffed or under-skilled IT personnel.

Information security and business continuity readiness is now an executive priority. Why? Leaders have a fiduciary responsibility to protect their organization and its assets. Now, information security is a priority not just for IT, but also for executives and their Boards of Directors.

Regulatory bodies such as the Security & Exchange Commission (SEC) and the Federal Trade Commission (FTC) have revised their information security requirements for organizations under their jurisdiction. Additionally, insurance companies, vendors and potential customers are vetting information protection practices.

As executives sign attestation letters around information security practices, they are requiring more validation and transparency. Same for auditors. Add to that a new set of state-level regulations to protect consumer data, and it's clear: it's time to get serious about implementing more holistic information security practices.

WHAT DOES A REASONABLE SECURITY PROGRAM LOOK LIKE?

There are nine elements that a good information security program must include. Let's look at each element, step by step.

1 DESIGNATE A QUALIFIED INDIVIDUAL TO IMPLEMENT AND SUPERVISE YOUR INFORMATION SECURITY PROGRAM.

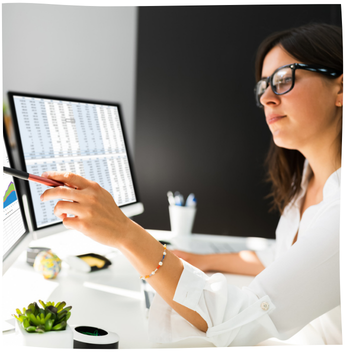
The Qualified Individual can be an employee of your company or can work for an affiliate or service provider. The person doesn't need a particular degree or title. What matters is real-world know-how suited to your circumstances. If your company uses a service provider for this function, the buck still stops with you. You must designate a senior employee to oversee this activity.

If the Qualified Individual works for an affiliate or service provider, their company must also maintain an information security program.

2 CONDUCT A RISK ASSESSMENT.

You can't formulate an effective information security program until you know what information you have, and where it's stored.

After completing your inventory, conduct an assessment to determine foreseeable risks and threats (internal and external) to the security, confidentiality, and integrity of customer information.



The risk assessment must be written and must include criteria for evaluating those risks and threats. Think through how information could be disclosed without authorization, misused, altered, or destroyed. The risks to information constantly morph and mutate, so you need to conduct periodic reassessments considering changes to your operations or the emergence of new threats.

3 DESIGN & IMPLEMENT SAFEGUARDS TO CONTROL THE RISKS IDENTIFIED THROUGH YOUR RISK ASSESSMENT

In designing your information security program, your plans need to address the following:

- **Implement and periodically review access controls.** Determine who has access to what kinds of information and reconsider on a regular basis whether they still have a legitimate business need for it.

- **Know what you have and where you have it.** A fundamental step to effective security is understanding your company's information ecosystem. Conduct a periodic inventory of data, noting where it's collected, stored, or transmitted. Keep an accurate list of all systems, devices, platforms, and personnel. Design your safeguards to respond with resilience.

- **Encrypt customer information on your system and when it's in transit.** If it's not feasible to useencryption, secure it by using effective alternative controls approved by the Qualified Individual who supervises your information security program.

- **Assess your apps.** If your company develops its own apps to store, access, or transmit customer information; or if you use third-party apps for those purposes, implement procedures for evaluating their security.

3 DESIGN & IMPLEMENT SAFEGUARDS TO CONTROL THE RISKS IDENTIFIED THROUGH YOUR RISK ASSESSMENT (CONTINUED)

- **Implement multi-factor authentication for anyone accessing customer information on your system.** For multi-factor authentication, best practices require at least two of these authentication factors: a knowledge factor (for example, a password); a possession factor (for example, a token), and an inherence factor (for example, biometric characteristics). The only exception would be if your Qualified Individual has approved in writing the use of another equivalent form of secure access controls.

- **Dispose of customer information securely.** Establish retention policies and deploy systems to securely manage the data according to the policies. It is particularly important to dispose of unnecessary data; while also retaining other information based on business need or legal requirement. This can be complex, and can no longer be done via a manual process.

- **Anticipate and evaluate changes to your information system or network**. Changes to a network can undermine existing security measures. For example, if your company adds a new application, has that created a new security risk? Because your systems and networks change to accommodate new business processes, your safeguards can't be static. The change management must be part of your information security program.

- **Maintain a log of authorized users' activity and watch for unauthorized access**. Implement procedures and controls to monitor when authorized users are accessing customer information on your system and to detect unauthorized access.

4 REGULARLY MONITOR AND TEST THE EFFECTIVENESS OF YOUR SAFEGUARDS

Test your procedures for detecting actual and attempted attacks. Testing can be accomplished through continuous monitoring of your system. If you don't implement that, you must conduct annual penetration testing, as well as vulnerability assessments, including system-wide scans every six months designed to test for publicly known security vulnerabilities. In addition, test whenever there are material changes to your operations or business arrangements and whenever there are circumstances you believe may have a material impact on your information security program.

5 TRAIN YOUR STAFF

A security program is only as effective as its least vigilant staff member. Employees trained to spot risks can positively multiply the impact of a program. Provide your people with security awareness training and schedule regular refreshers. Insist on specialized training for everyone (internal or external) with hands-on responsibility for carrying out your information security program.

6 MONITOR YOUR SERVICE PROVIDERS

Select service providers with the skills and experience to maintain appropriate safeguards. Your contracts must spell out your security expectations, build in ways to monitor your service provider’s work, and provide for periodic reassessments of their suitability for the job.

7 KEEP YOUR SECURITY PROGRAM CURRENT

The only constant in information security is change: changes to your operations, changes based on risk assessments, changes due to emerging threats, changes in personnel, and changes necessitated by other circumstances you believe may have a material impact on your information security. The best programs are flexible enough to accommodate periodic modifications.

8 CREATE A WRITTEN INCIDENT RESPONSE PLAN

Every business needs a response and recovery plan in place in case it experiences a "Security Event". A Security Event is an episode resulting in unauthorized access to or misuse of information held by your organization. Your response plan must cover:

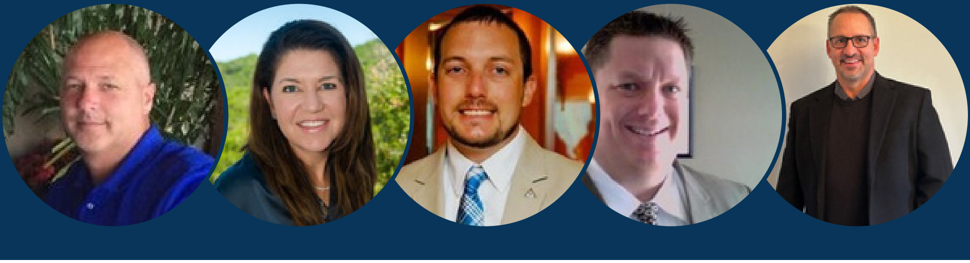
- The goals of your plan;
- The internal processes your company will activate in response to a Security Event;
- Clear roles, responsibilities, and levels of decision-making authority;
- Communications and information sharing both inside and outside your company;
- A process to fix any identified weaknesses in your systems and controls;
- Procedures for documenting and reporting Security Events and your company's response; and
- A postmortem of what happened and a revision of your incident response plan and information security program based on what you learned.

9 REQUIRE YOUR QUALIFIED INDIVIDUAL TO REPORT TO YOUR BOARD OF DIRECTORS

Your Qualified Individual must report in writing regularly, and at least annually, to your Board of Directors. If your company doesn't have a Board or its equivalent, the report must go to a senior officer responsible for your information security program.

The report must include an overall assessment of your company's compliance with its information security program. In addition, it must cover specific topics related to the program, for example, risk assessment, risk management and control decisions, service provider arrangements, test results, security events, how management responded, and recommendations for changes in the information security program.

Our team ensures your IT systems mean business.



NEXT STEPS

These best practices provide a clear framework for how all organizations need to address information security and business continuity.

Taking a more structured and, in many cases, auditable approach, will help your organization address supply chain reviews, insurance questionnaires and create a competitive advantage when securing new business.

Advanced Logic has moved through these exact stages to meet audited standards such as SOC-2. We understand the operational challenges as well as the technical standards.

Navigating the increasing standards for accountable, engaged systems security is critical for business continuity. But it does not have to be overwhelming. Our leadership team can help you navigate the challenges.

If you’d like to discuss your needs or questions about your data security and business continuity strategies, we're happy to set up a no-obligation call.

Contact us at (800) A TEAM4U or schedule a call today!

Schedule a Call