PERRY JOHNSON REGISTRARS, INC.

Business Resilience Through Cybersecurity

The growing importance of protecting your organization and its customers from cybersecurity threats is undeniable. From ransomware attacks to the theft of personal data, hackers and other bad actors can easily reach around the globe to harm a business without getting out of their chair. In addition to the relative ease of such attacks, exploiting cybersecurity weaknesses can also be incredibly lucrative and quick. Compared to, for instance, stealing a credit card from someone's wallet (which is quickly detected and easily blocked), stealing personal information via the internet can enable the thief to have new cards issued under their name, or – on a larger scale – a thief could target a database filled with thousands upon thousands of customer names and credit card information. Because almost every business deals with sensitive information in some way, shape, or form, it is important for players in every industry to protect itself, and its customers, by investing in cybersecurity.

Cybersecurity measures address threats to information assets and computer systems in three areas: confidentiality, integrity, and availability. Confidentiality includes the methods by which assets and systems are only available to authorized individuals, and protected from those without permission. Integrity concerns the complete, accurate, and up-to-date nature of assets and systems. Finally, availability includes the ready availability of necessary assets and systems to authorized users at any time as necessary.

Establishing a resilient cybersecurity plan begins, as with any system intended to reduce the threat of loss or failure, with a thorough risk assessment. Identifying which measures should be implemented and with what degree of intensity will lay the foundation of the system to be built on top. Evaluate your organization's threats and vulnerabilities – ask who, what, why, and how-type questions: “Who may target us?” “What will they target?” “How will they obtain their goal?” The answers to these can get you started along the way to identifying weaknesses. It's important to also remember that regulatory or contractual requirements may also influence your priorities when identifying risk; make sure you're aware of these and take them into consideration.

Once risks have been identified, there are several ways to respond:

- By **treating** risk, you may implement a measure (or several measures) to reduce the chance or the impact of said risk.
- By **terminating** risk, you eliminate the risk at the source.
- By **transferring** risk, you pass the responsibility for said risk on to another party, such as outsourcing to a third party or taking on insurance.
- By **tolerating** risk, you elect to retain the risk – perhaps because there is no viable way to effectively treat it or because the risk has been deemed acceptable.

Because there is no 100% guarantee of an implemented measure being effective every single time a threat appears, a treated risk should still be considered an active risk – it has not been eliminated, simply made less likely or less harmful. A deference-in-depth approach can help address the remaining "cracks in the shield," so to speak, offering a more nuanced, layered protection. Ideally, each part of this plan will present a range of different challenges for attackers to overcome, rather than all relying on the same type of security. A security plan is only as strong as its weakest link; find and strengthen this point – depending on what types of attacker seem most probable – and help mitigate the risk.

Alongside the three facets of security (confidentiality, integrity, and availability), it's important to take into consideration the three factors of defenses that must be covered: people, processes, and technology. It's common for organizations to focus solely on implementing technology or software solutions, and to neglect the human component of a security framework. The programs and hardware involved must be implemented and maintained by people; don't forget about them! Likewise important are the processes followed by the humans maintaining the security framework. Thorough, sound processes that are documented and regularly scheduled are crucial. Finally, technology is the most obvious of the three, even if they are imperfect and reliant upon the human factor.

Resilience also includes being able to handle an incident once it occurs – and in cybersecurity the first step in doing so is *detecting* that a breach has occurred in the first place. Detective measures fall into three categories:

- Pre-incident detection may be considered a form of prevention, taking appropriate precautions before an attack can take place. This can include vulnerability scanning or penetration testing.
- Real-time detection kicks in when preventive measures have failed and an attack has been successful. Automatic notifications, an alarm going off on a breached door, and other forms of warning are included in this category.
- Post-incident detection is unfortunately common, as many incidents are discovered long after the fact. Regardless of the security failure, it is important to be aware that an attack took place and was successful, in order to follow up with damage limitation.

The response to an attack rounds out a company's resilience, covering methods chosen to identify, contain, eradicate, and recover from an attack. The lessons learned from a cybersecurity failure offer an opportunity to improve that is as invaluable as a strong security system to start.

For more information, reach out to PJR – call **(248) 358-3388** or email **pjr@pjr.com**.