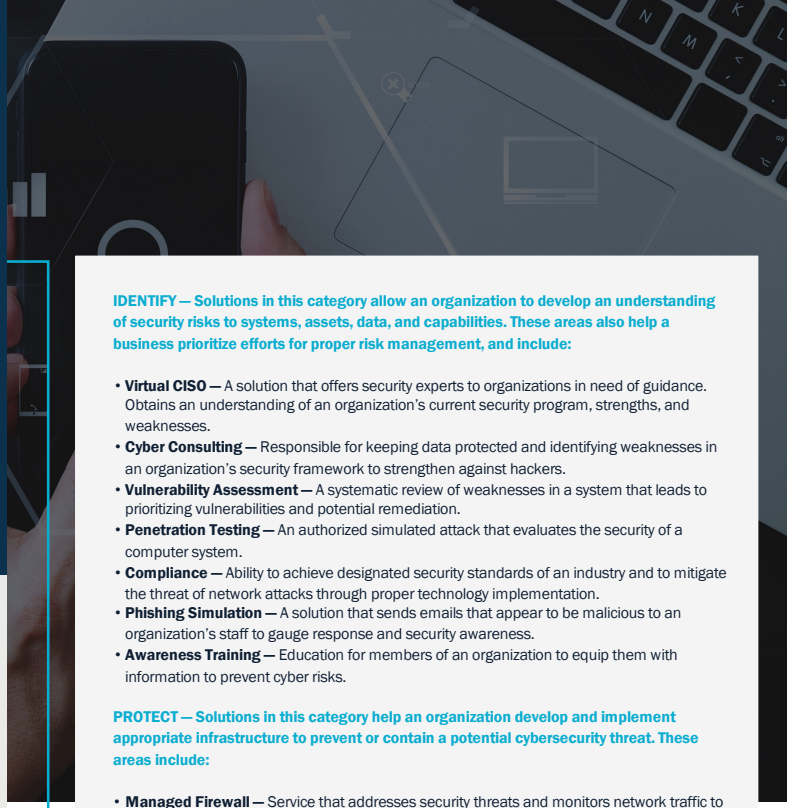

A TRUSTED TECHNOLOGY PARTNER FOR YOUR SECURITY NEEDS

Digital environments are becoming more complex as businesses manage remote workforces and now security has become more than having a firewall in place and a locked front door. The risks are too huge to ignore, from small businesses getting attacked daily to enterprises making front-page headlines for data breaches. Both financial losses and reputations are at stake. All of this has played a part in what has become a rapidly growing technology market — Gartner estimates that organizations worldwide will invest $133.7 billion by 2022.

According to the FBI, these are the five most common cybersecurity risks and crimes your organization could face without proper protection:

- Spoofing and phishing
- Business email compromise
- Identity theft
- Ransomware
- Online predators

Security requires an holistic approach that encompasses both technology and the human element that interacts with it. The crucial elements that make up the world of security can be organized into the categories of: technical solutions; the processes to evaluate and react to potential threats/vulnerabilities/impacts; and user training/education.

Outside Threats to Consider

Any organization could benefit from using well developed cybersecurity platforms and habits. Every company needs some form or factor of cybersecurity in order to compete in the modern age.

Regardless of your security needs or industry regulatory compliance you're trying to abide by, we're here to help you. Whether you're looking for security technology to help you identify, protect, detect, or respond to threats, we offer a full set of providers and solutions to meet your individual needs and combat the growing number of cyber threats organizations face.

Perimeter Security | Network Security | Endpoint Security | Application Security | Data Security

IDENTIFY — Solutions in this category allow an organization to develop an understanding of security risks to systems, assets, data, and capabilities. These areas also help a business prioritize efforts for proper risk management, and include:

- **Virtual CISO —** A solution that offers security experts to organizations in need of guidance. Obtains an understanding of an organization's current security program, strengths, and weaknesses.
- **Cyber Consulting —** Responsible for keeping data protected and identifying weaknesses in an organization's security framework to strengthen against hackers.
- **Vulnerability Assessment —** A systematic review of weaknesses in a system that leads to prioritizing vulnerabilities and potential remediation.
- **Penetration Testing —** An authorized simulated attack that evaluates the security of a computer system.
- **Compliance —** Ability to achieve designated security standards of an industry and to mitigate the threat of network attacks through proper technology implementation.
- **Phishing Simulation —** A solution that sends emails that appear to be malicious to an organization's staff to gauge response and security awareness.
- **Awareness Training —** Education for members of an organization to equip them with information to prevent cyber risks.

PROTECT — Solutions in this category help an organization develop and implement appropriate infrastructure to prevent or contain a potential cybersecurity threat. These areas include:

- **Managed Firewall —** Service that addresses security threats and monitors network traffic to adjust accordingly for optimal protection.
- **Web Security —** Applications that are implemented to ensure website data is not vulnerable to cyber risk or crime.
- **Email Security —** Solutions that protect email accounts and their content from cyber attacks and unauthorized access.
- **Endpoint Security —** Securing endpoints or entry points of end-user devices to prevent a security breach or threat.
- **Managed Cloud Firewall —** Software built to stop or mitigate unwanted access to private networks.
- **Data Protection —** Solution that safeguards important information from compromise or loss.
- **Zero-Trust Framework —** A framework that prevents data breaches by removing the concept of trust from the network architecture of an organization.
- **Remote User VPN —** Solution that allows a user to connect to a private network from a remote location as if they were plugged into an organization's network server.
- **Patch Management —** Application that distributes and implements updates to a software to correct any vulnerabilities for increased security.
- **SIEM —** System that collects, stores, investigates, supports, mitigates, and reports on security data for incident response, forensics, and regulatory compliance.
- **SASE —** Framework that applies SD-WAN with security to enable cloud adoption and the ability for organizations to apply secure no matter the location of users.
- **VPN —** Encrypted connection over the internet from a device to a network, allowing sensitive data to be safely transmitted.

DETECT — Solutions in this category carry out appropriate actions to identify a cybersecurity threat or occurrence. These areas help with timely threat and risk discovery, and include:

- **AI Machine Learning —** Detection of threats by artificial intelligence to stop threats.
- **Intrusion Detection —** Solution that monitors a network for malicious activity, which is then reported if detected.
- **Intrusion Prevention —** Threat prevention technology that continuously examines network traffic flows to detect security vulnerabilities.
- **SOCaaS —** Software-based service that offers a team of outside security experts to pinpoint threats.

RESPOND — Solutions in this category take action in the event of a detected threat or security attack. These areas include:

- **Incident Response —** Approach to contain and recover from a security breach or event.
- **Containment, Eradication, and Restore —** Interaction with compromised system in a way that helps restore and that prevents further damage.

Stephen McGarry
President
smcgarry@mcgarryconsulting.com
312-283-4295

Consulting Group