WHITEPAPER

OMNIA® PARTNERS

Purchasing Cybersecurity Tools and Solutions

PROTECTING YOUR GREATEST ASSETS FROM THREATS

Each day it becomes more evident that we are living in the age of the internet. Most people keep at least one device on their person at all times, using their face, fingerprints, and personal information to access their devices, company networks, social media sites, and various third-party websites. While recent technological advancements have boosted our productivity and ability to connect, they have also opened new avenues for attackers to compromise data, especially the data of more sensitive organizations. A quick glance at the news shows not only the latest innovations in technology and AI, but also the rising frequency of ransomware attacks that cost major organizations millions, as well as everyday individuals falling victim to scams that jeopardize their bank accounts and identities.

Although high-profile cyberattacks often make the headlines, it's important to remember that no agency or organization is completely immune from these attacks. K-12 public school administrators may need to better secure both paper student records and classroom learning devices. Local and state government officials could focus on safeguarding citizens' personal information. Corporate and enterprise organizations may prioritize defending against phishing scams and training employees to recognize and avoid these threats. The procurement functions of these organizations must be involved in preventative initiatives, since protecting against attacks often requires new products and solutions.

Global cybercrime costs are increasing rapidly and are expected to hit $10.5 trillion by 2025. These costs can stem from damaged, destroyed, or stolen data, as well as from productivity and reputation losses, business continuity disruptions, fraud, and post-incident activities such as investigations and restorations.[1] Regardless of your industry, procuring the right solutions to secure your assets is essential in today's volatile cybersecurity climate to ensure your organization can effectively combat and recover from cybercrime and other IT-related incidents.

Read on to find out how a strong procurement strategy can protect your organization from cyber threats.

PURCHASING CYBERSECURITY TOOLS AND SOLUTIONS

Despite the growing rate of cyber incidents that affect organizations worldwide, global spending on cybersecurity services and solutions is also rising. Organizations are using their funds to safeguard devices, consumers, and overall operations more than ever, and cybersecurity spending is now projected to total $1.75 trillion for the period from 2021–2025.[1]

When searching for IT solutions to add to your arsenal, your pain points probably center around quality, speed, and agility. The solutions must be effective enough to thwart attackers, implemented in a timely manner, and adaptable to organization needs.

As you consider how your own organization's procurement function can focus on security needs, it's important to know the solutions you need to prevent, identify, and recover from threats to your physical facilities, devices, virtual systems, and the people who use them.

CYBERSECURITY SPENDING IS NOW PROJECTED TO TOTAL $1.75 TRILLION FOR THE PERIOD FROM 2021–2025

PHYSICAL FACILITIES

The number of people working and learning remotely is steadily increasing, but you must still prioritize the security of physical facilities and on-site infrastructure as you budget for upgrades. Whether you manage a higher education institution with cameras to identify intruders or run an enterprise business with a web application hosted on on-premises servers, your operations rely on secure and functional physical infrastructure.

PREVENT

Outfitting your organization to withstand every potential physical threat may sound ideal, but it's impossible to fully prepare for the unknown. Start by collaborating with your personnel and stakeholders to determine the threats most likely to impact your facility. Then evaluate the likelihood of the threats to occur and the impact they could have on your operations. Finally, for the risks you identify, name the solutions in place to mitigate those risks.[2]

Solution & best practice recommendations:

- Fences or landscape-based barriers to secure the outer perimeter of a property
- Bollards to protect schools, government facilities, and other buildings from vehicle damage
- Reinforced doors and windows to protect buildings from debris and attackers
- Electronic locks to ensure doors lock automatically when necessary
- Turnstiles that only allow one person to enter a facility at a time
- Badge or biometric access systems to keep unauthorized individuals out of secure areas
- Visitor management technology to log people entering and exiting the premises

IDENTIFY

It's also important to implement measures to identify threats that are either actively occurring or about to occur. And, especially for organizations with a lot of personnel or sensitive institutions like schools, take time to think about the process for notifying facility occupants and first responders of an incident and how first responders can access your facility during an emergency.[2] Properly implementing these plans is a great start to protecting the people who rely on you.

Solution & best practice recommendations:

- Security guards to patrol secure buildings and monitor for intruders
- CCTV cameras for real-time monitoring and recording of activities
- Motion sensors to detect movement in sensitive or restricted areas
- Alarm systems to trigger alerts for unauthorized facility access or suspicious activity
- Smoke detectors and fire alarms to detect and alert occupants of fires
- Flood sensors to detect water leaks or flooding
- Temperature and humidity monitors in areas like server rooms to protect equipment

RECOVER

Solutions to prevent and identify threats to a facility can be effective, but you should also establish plans to return to normal operations after an incident occurs. This may include plans on where personnel should resume work after an office fire, or how power is restored to a school after a power outage.

Solution & best practice recommendations:

- First aid kits to handle medical emergencies
- Evacuation signage to guide occupants safely out of a building
- Emergency lighting to provide illumination during power outages
- Generators to supply backup power and keep essential systems operational
- Uninterruptible power supply (UPS) systems to supply power for critical devices
- Notification systems to alert building occupants and stakeholders of recovery updates

DEVICES

Organizations depend on a wide range of devices to function effectively, and these devices are often used by their stakeholders. For instance, K-12 and higher education institutions utilize everything from computer labs to televisions and education technology to enhance student learning. Businesses and government agencies provide employees with laptops, monitors, and other useful equipment. Ensuring the security of these devices is essential, since one device infected with malware or ransomware can compromise the integrity of the rest of your network.

PREVENT

Before you can effectively prevent viruses and other bad actors from impacting your organization's devices, you must familiarize yourself with the devices that access your network. You may already manage devices that are given to students and employees, but what standards have you established for smartphones that employees connect to your Wi-Fi? How do you secure Internet of Things (IoT) devices—such as smart home devices, wearable devices, and other interconnected gadgets—that give attackers more ways to access shared data and breach systems?[3]

Solution & best practice recommendations:

- Mobile device management (MDM) solutions to manage and secure devices
- Updates to operating systems, applications, and firmware to protect against vulnerabilities
- Patch management solutions to ensure software is updated systematically and promptly
- Updated antivirus and anti-malware solutions that provide real-time protection
- Full disk encryption on all devices to protect data in case of theft
- Virtual private network (VPN) services to secure remote network connections
- IoT security solutions for IoT devices connected to the network

IDENTIFY

Ransomware, a type of malware that denies access to a computer system until a ransom is paid, poses one of the biggest risks to devices. In fact, ransomware attacks are projected to impact companies, government agencies, consumers, and devices every two seconds by 2031 with damage costs exceeding $265 billion.[1] Other threats come in the form of viruses, zero-day exploits of software and hardware vulnerabilities, and denial of service (DoS) attacks that can overwhelm a device with traffic. It is vital to identify these risks before they impact your devices.

Solution & best practice recommendations:

- Firewalls that can help block unauthorized access to your devices
- Periodic antivirus scans to detect and remove any malicious software
- Endpoint detection and response (EDR) solutions to respond to suspicious activity
- Security audits and vulnerability assessments to identify and address weaknesses
- Comprehensive logging and monitoring to detect unauthorized activity
- Behavioral analysis tools that alert to irregular user activity

RECOVER

In the event that one or multiple of your organization's devices become infected, it is crucial to implement measures to quarantine the affected device from the remainder of the network, restore any lost or damaged data, and prevent similar future incidents.

Solution & best practice recommendations:

- Virtual local area networks (VLANs) that can limit the device's impact on the network
- System reinstallation procedures to restore heavily infected systems
- Incident response plan documentation to guide and manage the recovery process
- Forensic analysis to identify compromised data and gather evidence for further action
- Post-incident reviews to analyze the attack, response efficacy, and areas for improvement
- Regular backups of critical systems that can be used to recover data

VIRTUAL SYSTEMS

There are many benefits to using the cloud instead of physical IT infrastructure, such as enhanced IT productivity, agility, and scalability.[4] Organizations and individuals alike are recognizing these benefits and increasingly turning to the cloud for storage, software as a service (SaaS) tools, application development and testing, website and application hosting, and computing resources. In fact, by 2025, the amount of data stored in the cloud is projected to reach 100 zettabytes.[1]

More data in the cloud means more attackers are trying to breach the systems maintaining this data. Many cybercriminals engage in identity-based attacks, such as man-in-the-middle attacks, where a network connection is intercepted; credential snuffing, where stolen credentials are used to access account information; or password spraying where common passwords are used to attempt logins across multiple accounts. DoS attacks are also a threat and can completely shut down an organization's network with a flood of illegitimate traffic.[5]

PREVENT

An important step in preventing cybercriminals from disrupting your virtual assets is implementing zero trust principles, which require users, devices, and applications to continually verify their identity and access permissions. The zero trust model should also be coupled with the principle of least privilege, which requires users and assets to be granted the minimum access necessary to perform their duties.[6] Other preventative solutions will depend on your organization's unique system-related risks.

Solution & best practice recommendations:

- Role-based access controls (RBAC) to establish user roles with specific permissions
- Multi-factor authentication (MFA) requirements for accessing systems
- Centralized management solution that allows system administrators to control remote access[6]
- Password policies that require users to create complex passwords and change them regularly
- Features from your cloud service provider like firewalls, DoS protection, and security groups
- Intrusion prevention systems (IPS) that are designed to detect and block anomalies
- Encryption protocols like HTTPS and VPNs for transmitting data, especially sensitive data
- Key management practices/managed services to ensure encryption keys are protected

IDENTIFY

Preventative measures can prove very successful in defending against cyberattacks, but organizations must also deploy solutions capable of detecting irregularities. Many of these tools offer additional analysis and response capabilities to help keep your cloud environment secure.

Solution & best practice recommendations:

- Firewalls that monitor and control incoming and outgoing network traffic
- Network monitoring tools that scan traffic patterns, bandwidth usage, and anomalies
- Intrusion detection systems (IDS) that monitor network traffic and alert to suspicious activity
- Logs from firewalls, servers, and applications that can be analyzed for any threats
- Cybersecurity solutions that are highly responsive and can detect failed login attempts[6]
- Security operations scenter (SOC) services to provide monitoring, analysis, and response
- Penetration testing to identify system weaknesses via simulated attacks

RECOVER

Effectively managing a security incident affecting your systems requires well-documented response strategies that clearly outline the roles and responsibilities of personnel involved in handling incidents. When creating incident response documentation, you need to have a plan that outlines the steps to follow if an incident occurs and who is responsible for following those steps. A great approach to designing one of these plans is to base it on an industry-standard framework, such as those from the National Institute of Standards & Technology (NIST) or the International Organization for Standardization (ISO).[7]

Another vital part of recovering from an incident is having robust backup policies and processes. All organizations have data to protect, whether it's of citizens served by a government agency, customers using a web application, or a company's own employees. If your organization has outdated backup operations, start with conducting regular backups for essential systems and securely storing the backups.[6] These backups should be tested at least annually to verify they can be used to restore systems.

PEOPLE

In many cases, cyberattacks on physical facilities, devices, and virtual systems can be traced back to phishing and social engineering (which often target internal users) or malicious employees misusing their access permissions. As generative AI continues to advance, attackers are increasingly leveraging these tools to craft more convincing phishing attempts. The sophistication of deepfake technology is also rising, allowing criminals to deceive employees and other stakeholders into divulging sensitive information.[3]

PREVENT

To protect your organization from the negative impacts of phishing and social engineering attacks, you must first understand the forms these attacks can take. Phishing scams can appear as deceptive emails, counterfeit websites, and intimidating phone calls designed to coerce or frighten the recipient. With emails, attackers may mimic those from well-known organizations, and the links within them may redirect victims to websites crafted by attackers. Additionally, phone calls may feature spoofed identities, creating a false sense of security for the victim.

Solution & best practice recommendations:

- Awareness of the latest phishing techniques and common red flags in phishing emails
- Training to educate employees on phishing tactics and signs of social engineering
- Phishing simulations to test employee responses and reinforce training
- Email filtering systems to detect and block suspicious emails
- Reporting tools employees can use to flag suspicious emails and calls

IDENTIFY

To identify phishing and social engineering attacks, you must educate those associated with your organization about scam characteristics. Teach employees, customers, students using personal devices at school, and government officials alike to scrutinize the sender's email address and the email content before taking any action. If a URL is included, advise them to hover over the link to preview it before clicking. If there's an unknown attachment, they should avoid downloading it. Instruct individuals on who to report suspicious messages to, ensuring that the proper authorities can investigate.

RECOVER

Phishing and social engineering attacks primarily target people rather than facilities, devices, or virtual systems, but the information attackers seek is often used to gain access to a site, device, or system. Once the perpetrator convinces an individual to click a link or disclose information, they can initiate further attacks using malicious software or by misusing the individual's information. Recovery from a successful phishing attack will require additional education and training, an analysis of the incident, execution of an incident response plan, access to system backups, and other best practices discussed in this whitepaper.

PROTECTING ASSETS WITH A GROUP PURCHASING ORGANIZATION (GPO)

Once you've assessed your organization's cybersecurity posture and identified gaps in how you protect your assets from attackers, the next challenge is purchasing the solutions that can effectively fill those gaps. While day-to-day IT purchasing needs can usually be met by your current IT supplier partners, strategic IT purchases—like those related to large cybersecurity projects—require a long-term plan and thorough vetting of supplier partners. Strategic IT purchases can take anywhere from 12-24 months from start to finish, but by engaging with a GPO, you can avoid 2/3 of that process.

The cost and compliance of IT goods and services may also be a roadblock for your organization. Though cybersecurity spending is increasing globally, many public institutions must still navigate state and federal procurement laws, which include guidelines on budget compliance, competitive bidding, vendor selection, and contract management. Similarly, purchasers at private institutions must adhere to internal budgets and mandates established by company executives. Partnering with a GPO can alleviate many of these concerns by ensuring a compliant procurement process and providing access to the products you need from the suppliers who best meet your needs.

OMNIA PARTNERS
AS YOUR ALLY IN PROCUREMENT

If you're looking for a GPO that can not only meet but exceed your cybersecurity needs, OMNIA Partners is committed to being your partner from start to finish. We can assist you in the solicitation and/or RFP processes, completing the contracting stage, understanding today's IT market, and managing the vendors serving you through our partner development program. With a free OMNIA Partners membership, you gain access to our extensive contract portfolio, which includes world-class managed service providers (MSPs) and value-added resellers (VARs) to support your IT needs on a national scale. Our suppliers can address nearly any cybersecurity need, from ransomware protection to cybersecurity education programs, while driving cost and operational efficiencies to help you comply with all necessary regulations.

Our IT-related portfolio offerings include:

- Hardware & Software
- Cybersecurity
- Unified Communications (UCaaS)
- Assistive Technology
- Data Storage & Management
- Facilities Technology
- Building Management Services
- Safety & Security Systems/Services
- Audio Visual (AV)
- Cloud Solutions
- Telecommunications
- & more.

Don't wait for a cybersecurity disaster to strike before implementing the necessary solutions to prevent, identify, and recover from attacks. Create documentation to prepare for multiple attack scenarios, research solutions to address any holes in your defenses, and educate individuals within your organization on how to spot attacks and stop attackers in their tracks. Visit our website today to explore our contract portfolio and discover the suppliers within our IT offerings. Select solutions tailored to your industry and business needs or connect directly with our subject matter experts (SMEs) that can walk alongside you in the purchasing process and serve as an addition to your team.

Partner with OMNIA Partners to save time and money while achieving your cybersecurity goals.

REFERENCES

1. https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/
2. https://www.cisa.gov/sites/default/files/2023-10/CISA_AASB_Security_Planning_Workbook_508_Compliant_20230929.pdf
3. https://www.forbes.com/sites/bernardmarr/2023/10/11/the-10-biggest-cyber-security-trends-in-2024-everyone-must-be-ready-for-now/
4. https://www.techtarget.com/searchsecurity/tip/Top-11-cloud-security-challenges-and-how-to-combat-them
5. https://www.forbes.com/advisor/business/what-is-cyber-attack/
6. https://www.cisa.gov/sites/default/files/2024-06/joint-guide-modern-approaches-to-secure-network-access-security-508c.pdf
7. https://www.techtarget.com/searchsecurity/tip/Incident-response-best-practices-for-your-organization