Edge

THE REGION'S NONPROFIT TECHNOLOGY PARTNER

Think Your Institution Is Not At Risk? Think again...

What every higher education administrator needs to know about third-party risks

WHITEPAPER

CONTENTS

EDGE IS SOCIAL!

Keep abreast on the latest Edge news, events, product and industry updates on your social media channel of choice. Follow or connect with us on:

Edge

@All_Things_Edge

@AllThingsEdge

855.832.EDGE (3343)

info@njedge.net

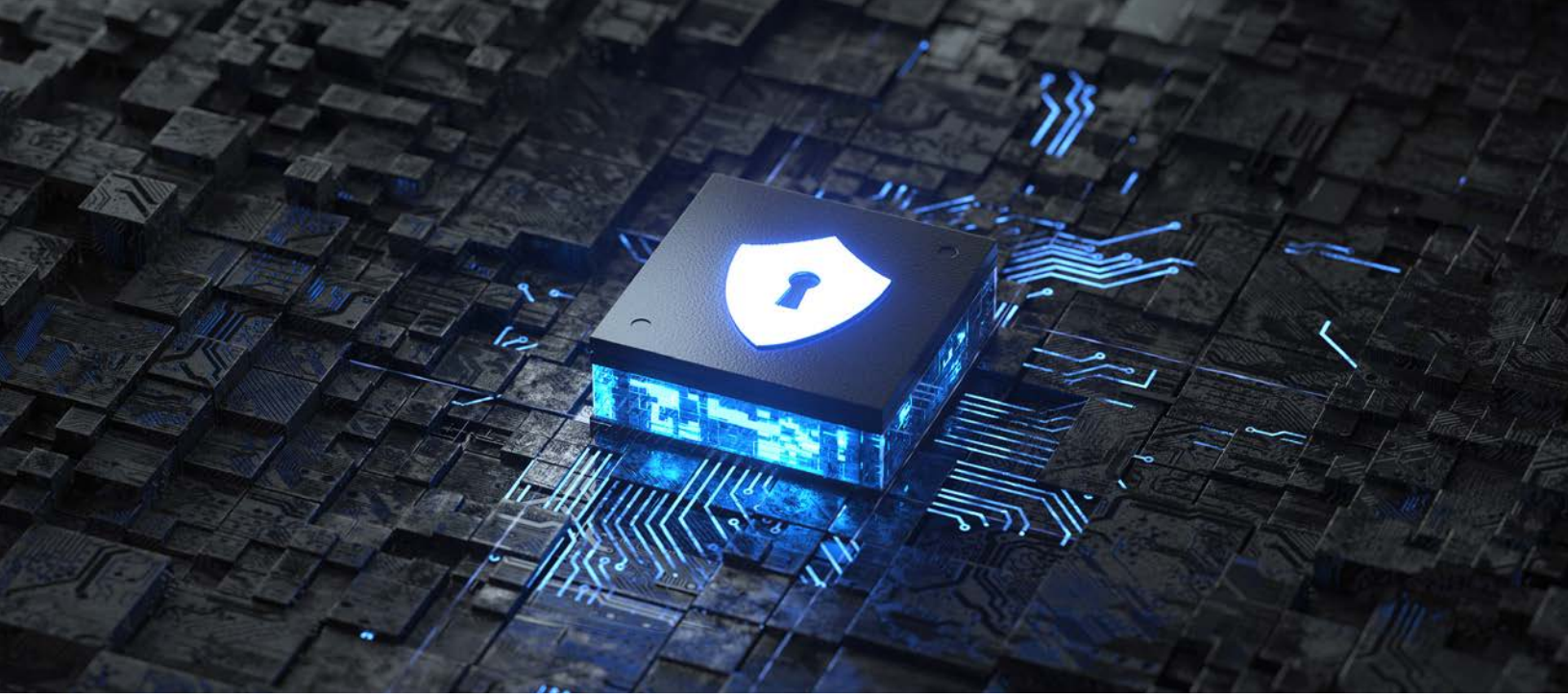
NJEdge.net

OUR LOCATIONS

Administrative Offices
625 Broad St, Suite 260
Newark, NJ 07102

Government Relations, Grants and Technology Advancement Offices
100 Overlook Center, Second Floor
Princeton, NJ 08540

Network Operations Center
1410 Wall Church Road Wall
Township, NJ 07719



Every large organization maintains agreements and contracts with third-party vendors to support and carry out daily operations on their behalf. This activity is also the case in colleges and universities that partner with vendors to deliver a wide variety of essential services, such as software solutions supporting students, faculty and staff. One recent Gartner report indicates that a median size organization contracts with nearly 5,000 third-parties. Seventy-two percent of institutional compliance leaders expect this number to increase by 2022.

While contracting third-party service providers can improve operations, enhance productivity, generate new revenue sources, and reduce costs, commercial vendors introduce a wide range of risks. *Developing effective third-party risk management is a mainstay of preventing cyberattacks and related expenses.* Given today's hyperconnected world, educational institutions must assess vendors and their security practices to better protect sensitive student and employee data.

HOW DID THE SOLARWINDS ATTACK OCCUR?

A state-sponsored hacker may have breached multiple public and private organizational networks through a popular SolarWinds software product. According to Reuters news agency, five people familiar with the SolarWinds attack revealed that suspected Chinese hackers exploited a flaw in the software, helping them break into computers and other systems.

Cybercriminals compromised SolarWinds's Orion solution that helps organizations manage their networks, servers, and networked endpoints. Cybersecurity experts believe that the cyber actor concealed malware inside Orion's software update. When installed, the malicious code enabled the hacker to perform reconnaissance, elevate user privileges, move to other environments, and compromise sensitive data.

Other news reports indicate that a group of Russian-backed government operatives used a software flaw to compromise approximately 18,000 SolarWinds customers, including federal agencies, by hijacking the Orion network monitoring software.

SolarWinds works with approximately 85 percent of Fortune 500 companies, 10 of the top US telecoms, the top five US accounting firms, *hundreds of universities and colleges globally*, and all US military branches. The SolarWinds breach's true scope might not yet be fully understood, but the event highlights that there are no doubts that hackers can attack even large commercial software vendors.

VENDOR RISK MANAGEMENT IN A POST-SOLARWINDS ENVIRONMENT

Indeed, the SolarWinds attack is a reminder of the importance of conducting risk assessments and due diligence before engaging vendors. The incident serves to caution all organizations partnering with vendors through outsourcing, especially for software services.

Institutions should be concerned about their data security, particularly sensitive student and staff data, as well as the Intellectual Property (IP) being developed in labs and centers. Currently, when a malicious attack will occur is difficult to predict, especially one with the scale and sophistication of a nation-state attack like the SolarWinds incident. In 2019, 44 percent of US companies experienced a significant data breach through a third-party vendor. Deloitte reported that 83 percent of organizations experienced a third-party incident in the past three years, with 11 percent causing a severe impact on customer finance, financial position, reputation, and regulatory compliance.

WHAT STEPS SHOULD EDUCATIONAL INSTITUTIONS TAKE TO MITIGATE VENDOR RISKS?

Clearly, multi-national bad actors are *targeting institutions of higher education.* Moving forward, educational institutions should focus on implementing procedures and policies to minimize the information accessed or disclosed to third-parties. A comprehensive vendor security management process that pinpoints and closes gaps in the cybersecurity strategy is essential.

Minimally, higher education institutions should implement the following controls to mitigate third-party risks:

1

Conduct In-Depth Due Diligence

Before outsourcing software services to a vendor, learning institutions should conduct thorough due diligence, either directly or through an experienced cybersecurity trusted partner. Indeed, outsourcing provides cost-savings, productivity, and efficiencies. However, introducing third-party systems on to company's networks introduces surfaces that cyber criminals may exploit. In that case, educational institutions should assess vendors' data security practices, past incidents, and other security audits the service provider conducts on its products. Organizations should implement due diligence procedures on all suppliers, including refined software companies.

Educational institutions engaging third-party service providers for any computing services to store, process, or share confidential data can conduct comprehensive security assessments using toolkits, such as the Higher Education Community Vendor Assessment Toolkit (HECVAT). HECVAT is a standard questionnaire that educational institutions can use to measure vendor risk and understand the security controls to protect confidential data.

2

Update Technical Controls

Maintaining the right enterprise-level security solutions is crucial. Educational institutions can prevent third-party risks by implementing "best practice" technical cybersecurity controls. For instance, insitutions can utilize multi-factor authentication to protect internal systems and devices. They can also implement reliable access control mechanisms to restrict third-parties from accessing information resources they do not need. Other technical security controls that organizations can consider include implementing encryption, backups, virtual private networks (VPNs), intrusion detection and prevention systems (IDS/IPS), and firewalls.

3

Contractual Commitment

Educational institutions should pay careful attention to the vendor's obligations when negotiating software agreements. Both parties should review and determine the steps to take and responsibilities in case of a cyber incident. Organizations should assess the vendor's notification provisions of suspected cybersecurity incidents. Both the educational institution and the third-parties should also engage in public-private-partnerships (PPPs) with government and industry to gain global threat intelligence and leverage collated information on best practices and standard approaches. PPPs offer ways that both the private and public sectors can collaborate and collectively create methods to counteract prevalent and emerging cyber threats.

4

Data Minimization

Even with a detailed due diligence procedure, vendors may fall victim to cyberattacks, as with the SolarWinds incident. Educational institutions should take care to minimize the amount and type of data they share with third-parties to limit data breach and legal obligations costs. Organizations can collaborate with vendors to develop and implement data minimization procedures to ensure an outsourced software only generates necessary information.

5

Awareness Training

Educational institutions should introduce security awareness training to bolster knowledge, improve behavior, and incentivize employees to practice good cybersecurity hygiene. Besides, organizations should develop and implement key security policies, such as an acceptable use policy, access control policy, information security policy, incident response policy, remote access policy, business continuity plan, and password policy.

6

Cybersecurity Insurance

Finally, educational institutions and software solutions vendors can agree on cybersecurity insurance policies to minimize third-party risks. Organizations can partner with suppliers to purchase a third-party cyber policy that pays for legal fees, settlements, and other costs in case of a data breach. However, take care that the policy is well understood and that the obligations and due diligence of both the institution and the third-party are met, lest the policy not cover a sticky situation when the time comes.

In reality, there is virtually no educational institution that does not outsource some activities, such as IT functionality, security, and software development, to an external service provider. The recent SolarWinds attack reveals the adage that there is no silver bullet for preventing sophisticated cyberattacks. Fortunately, educational institutions can implement the right measures, such as due diligence, contractual commitment, awareness training, data minimization, and cyber risk transfer to an insurance policy, to better understand and mitigate third-party risks.

In the past year Edge prevented or mitigated more than 495 cyber attacks against its members. Each day, Edge works with its members to assess, identify, remediate, prepare, and recover from institutional cyber attacks. To learn more, contact Edge at www.njedge.net/contact-edge/.

Edge.
THE REGION'S NONPROFIT TECHNOLOGY PARTNER