PARTNER CONTRIBUTED ARTICLE

Click to read the Spring 2021 issue of **NSCA *Integrate***

Why the SolarWinds Breach Hits Close to Home

By Rob Simopoulos

The high-profile SolarWinds hack is particularly relevant to NSCA members because it reminds us how cyber incidents can impact systems integrators and customers

It's still too early to know all the details of the **SolarWinds hack**, but what's been reported so far is that adversaries gained access to the company's development environment and altered Orion software code with the goal of providing a back door into the software users' systems.

By changing the code in this software (Orion), it has been estimated that thousands of users may have been targeted in the sophisticated supply chain attack; many may have been impacted. We will learn more as the investigation continues, but this is a strong reminder that cyberattacks are a potent and growing security threat. Adversaries are becoming more sophisticated in order to achieve their goals.

This attack showcases that cyber incidents don't impact only the company experiencing the breach—they have a **one-to-many impact** affecting vendors, customers, and partners. It's with this one-to-many scenario that you must remember: You have a need and responsibility to protect yourself with the ultimate goal of protecting other businesses as well.

Why Cybercriminals Could Target Integrators

What a systems integration firm does as a business is incredible: Connecting and integrating numerous disparate systems to achieve harmonious technology. But with this type of work comes significant cyber risk. We can't ignore the fact that integrators are a prime target for cyber criminals.

Integrators have a unique level of authorized access, which makes them prime targets for cybercriminals.

After the breach at SolarWinds, the entire world is looking at other firms and wondering how easily it could happen to them. We must view the systems integration industry in the same way.

Integrators have a unique level of authorized access, which makes you prime targets for cybercriminals:

- Systems integrators store sensitive information about their clients, including network topology and device layout diagrams, device passwords, floor plans to facilities, and MAC and IP addresses.
- With the growth of managed services, remote access to customer networks and systems has become commonplace. This practice makes managed service providers a target of cybersecurity adversaries; gaining access to remote management tools can give them a pivot point to many other organizations.
- Computers are the technician's tool of the trade; they move them between customer networks, plugging them in to program systems and devices. During a normal workday, a service technician could plug in to many different customer networks using the same computer, potentially putting each organization at risk if that device is infected.
- Many customer engagements are on a project basis, brought in and organized through general contractors. Once the technology is deployed, the integrator has no further responsibility. This quite often leaves systems unpatched and unmaintained in the customer's environment, potentially leaving vulnerable devices running and holes for attacks to occur.
- Systems integration projects come with high-dollar value, which makes them a target for business email compromise. Cybercriminals work to gain access to the finance person's email and, once accessed, the attacker can launch payment change requests toward their customers (and potentially have payments sent to them rather than to the integrator). With payment terms starting at 30 days, there is a lengthy time between these changes and collections processes, which can allow the criminal to be successful in their exploit without detection until much later.

These unique practices make you a tempting target for cybercriminals, especially knowing that a breach of one company (a systems integrator) could impact many others (customers, partners, and/or vendors).

Cybersecurity for Systems Integrators Requires Industry Evolution

The systems integration industry is amazing! I started in the industry at the age of 18 and have been part of it ever since, starting with analog systems and witnessing the change to digital and intelligent systems.

It's an industry that constantly improves, and I've seen how those who move *with* the advancements reap the benefits while those who do not are often left behind.

In my opinion, cybersecurity is the next step in the process of continuous improvement. It's the next essential digital pivot that systems integrators need to make. It's not a matter of consideration (to do it or not to do it), but a matter of evolving with the industry.

It's happening right here ... right now:

- Your customers have begun to select integrators based on cybersecurity posture.
- Vendor reviews and assessments now include a cybersecurity vetting process as a customer assesses to ensure providers have proper cybersecurity controls in place to protect them.
- Not advancing your cybersecurity posture will leave you failing these reviews and ultimately not winning the customer.
- Companies with strong cybersecurity posture and practices will enjoy growth; the others who don't make improvements will fade away.

Your customer provides you great power as they provide you with authorized access to their systems and information. Along with that privilege comes great responsibility: responsibility to do what's right and work to protect that privilege. Organizations will always be breached, even some with advanced cybersecurity controls in place. But, in a concerted effort, integrators can make it more difficult for adversaries to use the industry we know and love as a gateway into their trusting customers' systems.

*Rob Simopoulos is cofounder of Defendify, an **NSCA Business Accelerator** that provides cybersecurity consultation and solutions.*

WANT MORE?

Defendify offers NSCA members the Defendify Essentials Package: 3 free cybersecurity tools to help you know where you stand, where you might have gaps, and what's going on. Learn more here.

DEFENDIFY