# Contractor Cyber Risk Continues to Grow

## Learn how your organization can protect itself

### At a Glance:

- Third-party contractors are often overlooked when it comes to cyber risk
- Risks include malware, malicious activity, or human error
- Use these three strategies for risk mitigation
  - Contractor security policies
  - Network segmentation and entitlement management
  - Threat detection and response solutions

With increasing frequency, Arctic Wolf's team of security experts has responded to a new source of business cyber risk: third-party contractors.

Companies today seem comfortable inviting outside contractors onto their business sites and networks. These include contractors involved in hardware maintenance, as well as IT vendors, business consultants, and outside security consultants. Although businesses trust contractors with important network access permissions, contractors are proving to be a real cyberthreat.

**Examples from Arctic Wolf's security team include:**

- A printer technician's infected laptop began attacking local systems once hooked up to the printer needing repair
- At one company, a risk assessment consultant created unauthorized admin-level accounts in company systems to ease employee work responsibilities—but leave its customers less secure
- A security vendor brought in to make improvements misconfigured the client's IDS and firewall products, exposing the company to attacks

### Why Contractors Are Problematic for Cybersecurity

As businesses become more sophisticated about cybersecurity, it is not surprising that third-party contractors now pose a higher percentage of their cyber risk.

While IT departments work diligently to secure their network perimeters and monitor them for cyberattacks, contractors bring unsecured, third-party hardware to business sites and connect them directly to business systems. What's more, IT departments establish security policies and introduce specific tools to secure employee laptops and other devices, but contractors aren't required to comply with these policies.

Often, contractors are motivated to simply complete a task as quickly as possible and move along to the next customer. At times, this can lead contractors to act carelessly, cut corners, or violate security policies. To amplify the problem, businesses frequently lack qualified internal staff capable of reviewing a contractor's activities.

Many companies trust the reputation of the contractor's organization for protection. But Arctic Wolf security experts found contractor threats from leading companies across multiple industries. Businesses should not assume that contractors and their hardware are secure based on name recognition alone.

## Mitigating Contractor Cyber Risk

Contractors perform important business functions, and it is neither practical nor economical for companies to rely on in-house employees exclusively. Therefore, IT departments must develop strategies to mitigate cyber risk for contractors whom they employ.

**Three key practices are central to contractor risk mitigation.**

1. IT departments should establish security policies for outside contractors and communicate these policies. For example, the department can require that contractor laptops be scanned for vulnerabilities and malware using AV software to meet your company's IT hygiene standards.

2. IT should implement solutions that can control the scope of a contractor breach. Entitlement management solutions, which provide only fine-grained privileges to specific users, can prevent a contractor from accessing or impacting other business systems. Network segmentation is also key. Contractors should be restricted to company guest networks unless absolutely necessary.

3. IT should adopt a threat detection and response solution. These solutions continuously monitor a business's network and systems for anomalous activity. In the event that a contractor intentionally or inadvertently attacks or impacts a company's systems, the breach to be promptly discovered and remediated. This minimizes the business impact of a breach.

For many companies, a managed detection and response (MDR) solution such as AWN CyberSOC™ may be the best choice for detection and response. It lets companies take advantage of the business benefits of contractors, while affirmatively answering the question: "Am I safe from third-party cyber risk?"



SOC2 Type II Certified

**Contact us**
arcticwolf.com
1.888.272.8429
info@arcticwolf.com