ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

4 Ways to Mitigate Vendor Cybersecurity Incidents

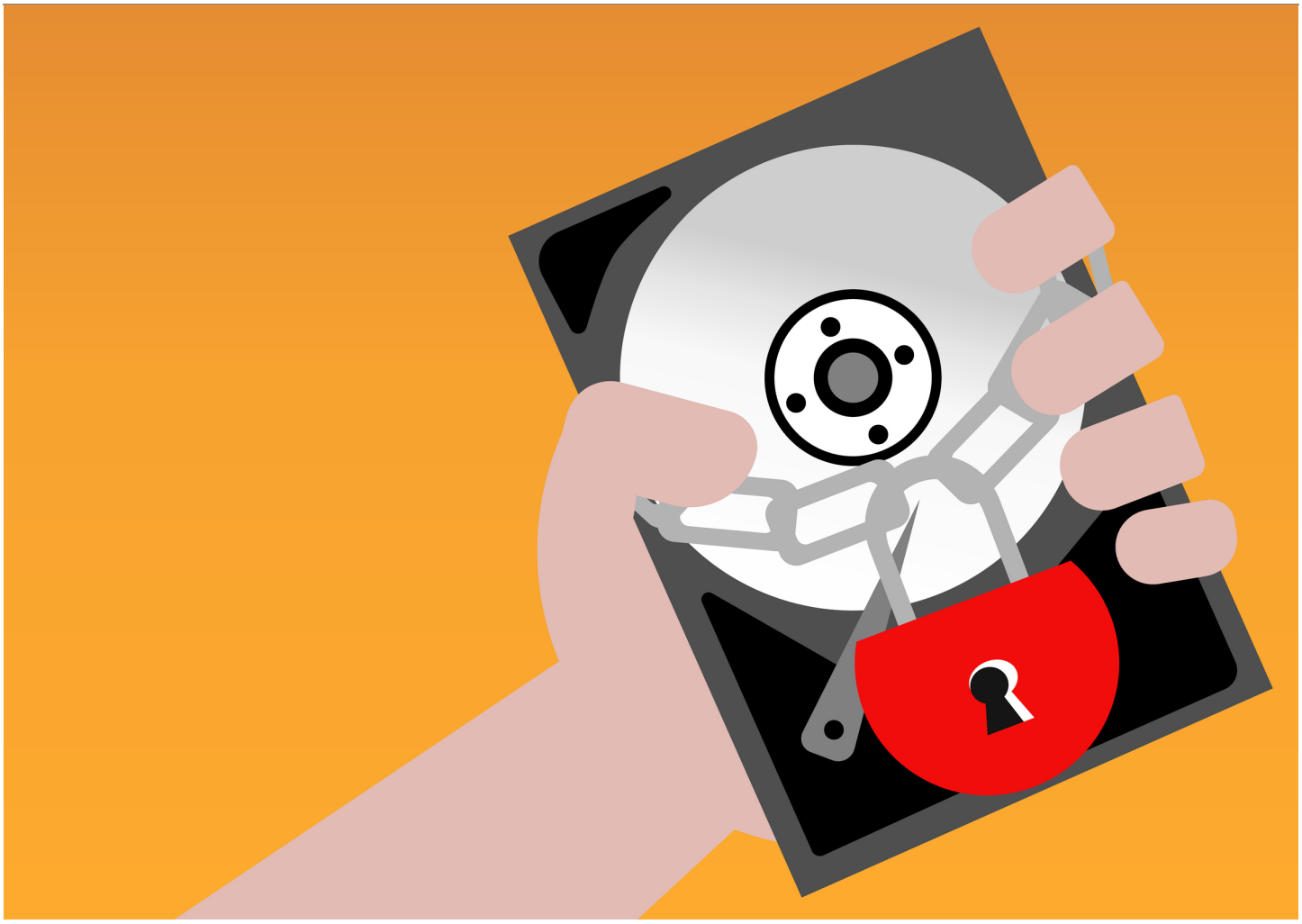
Technology, Privacy, and eCommerce

Banner artwork by Diyajyoti / *Shutterstock.com*

In May 2023, the CL0P ransomware gang wreaked havoc on more than 2,500 organizations by infiltrating Progress Software's MOVEit file transfer platform, stealing copious amounts of data and posting it on the dark web to extort ransom from affected companies. This single exploit resulted in millions of data breach notifications to individuals. It also sparked a host of lawsuits and prompted dozens of corporations to file public disclosures about risks associated with third-party vendors' use of MOVEit's platform. Moving into 2024, third-party vendor risk mitigation is taking center stage in the cybersecurity and data privacy context. This article explores how to attempt to address that risk.

1. Define expectations for early notification

Early notice about a vendor's incident is critical to managing the potential impact on your organization. To ensure timely notice, build robust incident notification requirements into your vendor contracts. We recommend notice provisions that require vendor incident notice within a specific timeframe — preferably a matter of hours but no more than three days after suspicion or discovery of an incident. Standard notice provisions typically state vendors will provide "reasonable" notice, but that definition could be up for debate after an incident.



Cyber criminals will use unsecure vendors as a gateway to your organization's data. Artwork by Bundit Yuwannasiri / *Shutterstock.com*

In ransomware incidents, cyber criminals may gain access to your organization’s information through your vendor and post that stolen information on the dark web. As such, early notice of potential exposure is critical to managing your organization’s regulatory concerns, crisis communications, and potential liability. Requiring notice within 24 or 36 hours — not just of an incident that impacts personally identifiable information — but of *any* incident that may impact *any* information belonging to your organization is an important step. Ensure your vendors alert you to an incident the moment they suspect your information is or could be compromised. Immediate notification affords an organization essential time to activate its own incident response plan.

> Ensure your vendors alert you to an incident the moment they suspect your information is or could be compromised.

2. Establish requirements for breach remediation

Robust contract requirements for vendor management of an incident also help mitigate risk. Include a provision requiring vendors to provide a certification from an outside forensic team of the “all clear” after a ransomware incident can alleviate disputes after an incident occurs about whether they have properly remediated a breach.

3. Insist on robust indemnification provisions

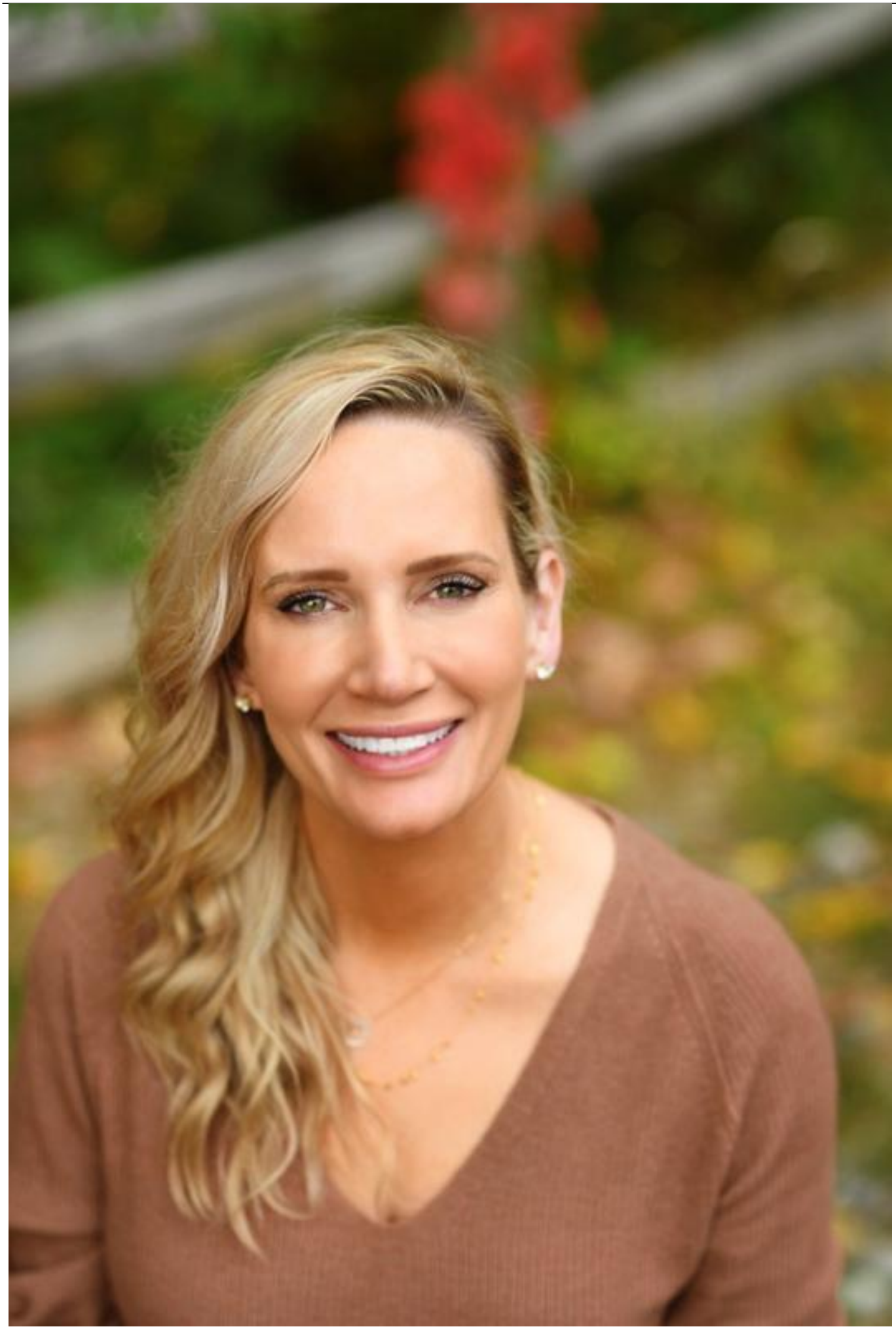
Vendor contracts often agree to cover the cost of consumer breach notices and credit monitoring, but these expenses constitute only a small percentage of the overall cost of an incident. Credit monitoring, for example, costs only cents on the dollar. Include robust indemnification provisions to your vendor contracts aimed at recouping the larger expenses your organization will face — lost profits, regulatory fines and penalties, crisis response, and outside attorneys' fees.

4. Assemble your own incident response team

One of the most important steps in-house legal teams can take is to make sure that when an incident occurs, their security teams know to notify the legal department. Seemingly minor breaches can quickly balloon into big issues. Assembling your own incident response team to address even a third-party breach can be critical to understanding whether the vendor's breach is critical to your own operations.

When notified of a potential vendor incident, set up a call with the vendor to learn more. Ask to speak directly with the forensic team involved in the incident. This allows you direct insight into what has occurred and what is being done to remedy a breach.

Kate Kreps

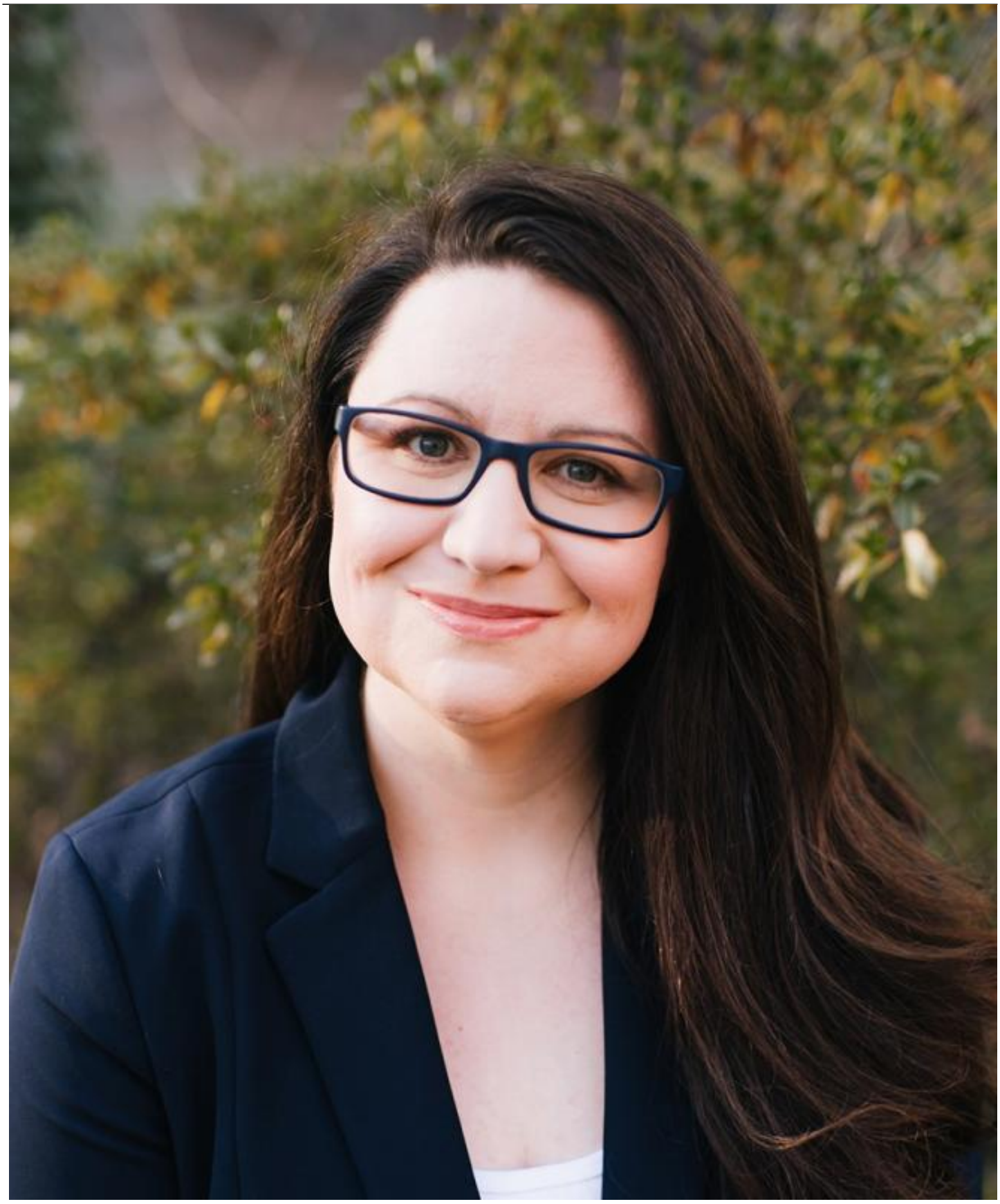


Chief Privacy Officer and Senior Counsel

American Electric Power

Kate Kreps is chief privacy officer and senior counsel at American Electric Power.

Elizabeth Burgin Waller



Principal and Chair of the Cybersecurity & Privacy Practice

Woods Rogers Vandeventer Black

Elizabeth Burgin Waller is a principal and chair of the Cybersecurity & Privacy Practice at Woods Rogers Vandeventer Black in Virginia.