Procurement Best Practices to Fight Against Cyber Attacks

The number of companies targeted by cyber attackers continues to soar. Companies like DocuSign, Equifax, and Uber – sophisticated companies with robust security teams and high standards for threat protection – have recently fallen victim to cyber security attacks.

Breaches like these have left us all wondering…are we doing enough to protect ourselves?

Access to sensitive internal, client, and supplier data puts procurement in a particularly vulnerable position. While IT and security must take the helm of developing a security solution that fits an organization's needs, procurement plays a unique role in strengthening an organization's security posture.

In this post, we'll explore the information procurement has at their disposal that makes them such a high value target, why they're increasingly susceptible to attacks, and best practices for ensuring organizations are protected.

What information does procurement have that hackers want?

Procurement is home to a plethora of valuable information, including but not limited to:

- Payment information, like credit cards, invoices, and bank account details
- Personal information, like W-9s, social security numbers, and contact information
- Company information, like bids, contracts, and confidential agreements

This information can be used by attackers for financial gain, identity theft, and to help competitors gain an advantage.

On the opposite side, cyber security breaches can be a huge headache for companies. Potential impacts include long-lasting damage to a company's reputation, revenue loss, valuable resources spent on crisis management and recovery, and more.

Why the growing focus on procurement as a target?

In an increasingly interconnected world, having easy access to the above information makes organizations more collaborative and efficient with suppliers, clients, and partners. While free-flowing information between these parties makes relationships far easier, it also poses critical

security risks.

The question plaguing many procurement professionals is how do they keep all of the great benefits that employees, clients, and suppliers alike have come to rely on, while still keeping the company secure?

What is procurement's role in preventing cybersecurity attacks?

Procurement can protect companies against cybersecurity risks in three main ways:

1. *Ensure that procurement employees are adequately trained* – Attackers have realized that they don't always have to hack into organization's back doors – they can enter right through the front when employees haven't been trained to use smart cybersecurity practices. Your organization will likely have its own standards. These should include best practices like:
    - Think before you click on links or attachments from unknown senders or from known senders that look suspicious.
    - Know the rules of encrypting information within your organization. Ask yourself, "Can this information be shared openly or should it be protected further?"
    - Always lock up your computer and clear your desk before leaving work.
    - Be careful of using public Wi-Fi and be mindful of the conversations you have in public.
    - Develop an awareness of cybersecurity risks. Understand the latest schemes that hackers are using and consider whether you are adequately protected.
2. *Develop standards for suppliers and enforce them* – There is no way to guarantee that the supplier you are working with has stringent cybersecurity standards. Without the right security measures in place, hackers could infiltrate your system through the channels you've set up to work more efficiently with suppliers. Standards should be set around the following areas:
    - How shared data is secured
    - Who can access it
    - What they can do with it
3. *Know the plan when an incident happens* – If you suspect that you have suffered a cybersecurity breach, your organization should have a published first response contact. This contact is typically either your manager, your security team, or your IT provider. Every moment counts during a cybersecurity attack, so raise the flag early.

Forbes called cybersecurity "the biggest concern of 2017" and with all of the attacks suffered this year, we don't see that changing in 2018. As the role of procurement continues to grow within organizations, so, too, should procurement's awareness of how to protect the valuable information they work with on a daily basis. Training procurement teams adequately on safe cybersecurity practices, implementing strict standards for suppliers, and having a clear cyber response plan will

help ensure that procurement plays an important role in strengthening a company’s security posture.

About **PurchaseControl**

PurchaseControl is cloud based procurement software for business spend management. We empower businesses by providing greater transparency and oversight into the purchasing process. With PurchaseControl, you have the flexibility to manage how spend actually happens instead of how you wish it would happen.

The entire PurchaseControl team has experience within a range of businesses, and as such, we bring a practical, holistic approach to purchasing. We understand what it takes to run a business and apply that knowledge to make PurchaseControl as effective as possible for all users.

Learn more at www.purchasecontrol.com

Contacts

EU Office Information

UK: +44 845 591 27 24

Ireland: +353 1 513 4623

enquiry@purchasecontrol.com

US Office Information

US: 800 737 5605

inquiry@purchasecontrol.com

Connect With Us

Facebook: https://www.facebook.com/PurchaseControl/

Twitter: https://twitter.com/purchasecontrol/

LinkedIn: https://www.linkedin.com/company/purchasecontol/