TITAN
CONSULTING
INSIGHTS

IS YOUR SAP ENVIRONMENT SAFE AND SECURE?

Align Your Security Strategy and Practices!

– Keith Johnson, Practice Manager

I'm sorry, your charge was declined. Do you have another card?"

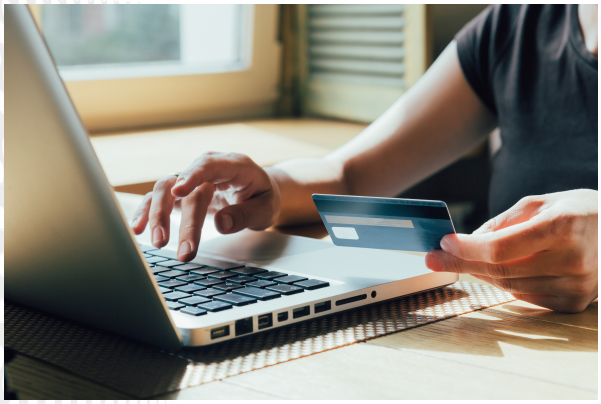
I was embarrassed and confused. I had just paid off that card. What was going on? I called the credit card company. After a brief hold, the representative explained: "We believe your card may have been compromised. We don't think your data was stolen, but as a precaution, we've issued a new card."

That made three compromised credit cards in just two years. It was frustrating and also eye-opening. If something as regulated and secure as a credit card account can be breached, **what about the vast and complex data sitting inside your SAP systems?**

Hackers are not just targeting individuals. They are going after businesses. If they can break into banks, they can break into your SAP system and access your most sensitive financial data.

So, what's the problem?

Hackers are increasingly targeting SAP data, for good reason. SAP systems drive nearly 74% of global business revenue, highlighting their critical role in the world's economy. Even more striking, 87% of the companies on the Forbes Global 2000 list rely on SAP to run their operations. With such widespread use among the largest enterprises, SAP systems have become a prime target for cyberattacks.



Recently, a breach occurred that forced a company to file for bankruptcy protection. The company, a federal contractor who performs background checks for the Department of Homeland Security (DHS), was hacked by overseas-sponsored hackers.

The breach occurred, and 25,000 DHS HR records were compromised. The records, hosted by a third party, contained personal and potentially compromising information. The contractor lost $2.8 billion in federal contracts, 2,500 people lost their jobs, and the company filed for bankruptcy. **All of this was a result of not protecting their SAP data and endpoints.**

This is one example of the devastating impact of the intentional theft of your confidential and proprietary data. There are many ways these crimes are committed, but the most common methods for compromising SAP data are:

- Access through Suppliers and Vendors
- Outsourced Processes and Applications
- Networks, Middleware (NetWeaver) and Endpoints
- Mobile Devices, Tablets, PC's
- ABAP and Custom Applications

In the DHS example above, the vulnerability resulted from a combination of factors. Hackers infiltrated a network belonging to one of the contractor's suppliers that stored ERP software. Because the partner's network was connected to the contractor's network, the attacker was able to move from the third-party environment into the company's systems by successfully brute-forcing a password on an application server.

Once the attackers gained access to that server, they installed a malicious backdoor that allowed them to reach the personnel records. Patience and time work in favor of the hackers unless you have a comprehensive strategy in place and execute it effectively.

The office of the Chief Information Security Officer (CISO) is challenged to prevent these thefts and protect the fiscal health of the company. SAP systems are one of their principal areas of focus since the company's most valuable data resides within SAP. For example, strategies, pricing values, products, sales figures, and trends all reside within your ERP systems.

From the PriceWaterhouseCoopers CEO Survey, cyber-crime is one of their top concerns. Most companies have a CISO and Strategy for cyber-security. **How does SAP fit into this strategy?**

Breaches are often traced back to business partners or vendors who may lack the size or resources to enforce strong security protocols. Recently, malware was introduced by a vendor into a global manufacturer's network when it was attached to data shared across their systems.

Middleware like NetWeaver is still a major target for cyberattacks. In early 2025, hackers took advantage of a serious vulnerability in NetWeaver's Visual Composer component. It allowed them to upload malicious files and run code on systems without needing to log in. They installed webshells, moved through internal networks, and stayed hidden while preparing for further attacks. SAP released a patch, but many systems stayed exposed for weeks.

This kind of breach is a reminder that hackers are patient. They can sit quietly inside your systems for over 100 days before launching their attack.

In SAP's defense, they fix these vulnerabilities as soon as they are aware of them. However, customer's practices are also to blame, such as not upgrading to the latest patches (OSS Notes). This is especially relevant to SAP customers that moved off SAP support to any third party software maintenance providers.

Since 2012, SAP has issued over 3,500 OSS Notes specifically related to security. Every month, on SAP's Critical Patch Day, which falls on the second Tuesday, SAP publishes one or more security advisories called SAP Notes. These notes provide details about newly discovered vulnerabilities or misconfigurations that could pose a risk to SAP systems.

SAP offers a range of tools to help IT departments detect and prevent breaches and vulnerabilities. At a recent ASUG Executive Exchange we sponsored, Anne Marie Colombo gave a presentation on SAP's Approach to Safeguard Your Business. If you would like a copy of the presentation or paper, please contact us directly through our website.

What you can do about it:

- Audit your systems and applications for potential risks and vulnerabilities.
- Confirm the security practices and protocols with your third parties and partners – and make them liable for breaches.
- Review custom applications, development and GUI's for vulnerabilities.
- Investigate and monitor access and endpoints at all locations.
- Apply Patches and OSS Notes frequently.

Is your data safe? Do you have good security practices? Titan Consulting is a leader in slashing IT costs and risks. If you have questions about Security Best Practices or how to improve your policies and procedures, contact your Titan Consulting Sales Director or visit our website at titanconsulting.net for more information.