Published on *The National Law Review* https://natlawreview.com

Could your ERP system make you a victim of cybercrime?

Article By:

Cameron Abbott

Allison Wallace

We frequently blog here about incidents where companies, government agencies or public have suffered data or security breaches at the hands of hackers. They're often incidents that come to light because they affect the public in some way – by shutting down hospitals, exposing sensitive personal information, or threatening government security. But what about hacks that, while not having wide-reaching public implications, go to the core of a business' operations?

A new survey has given an insight into the vulnerabilities companies running SAP or Oracle enterprise resource planning (**ERP**) software are facing – with 64% of respondents reporting a breach of their ERP systems in the past 2 years.

The information that was most sought after? **Sales data**. This was followed by personal information, IP and financial data. All information, if in the wrong hands, could destroy a company.

90% of SAP systems are reported to be vulnerable to 10KBLAZE, a public exploit discovered in April this year. The Oracle Payments module contains four critical bugs which require patching – if left unpatched, put sensitive data – including credit and bank account information – at risk.

If your business has an Oracle or SAP ERP system in place, how do you protect yourself? As a starting point, you should make sure you have in place robust cybersecurity and application maintenance policies and procedures. You should also make sure that included in those procedures is an audit process that truly assesses the system – identifying any vulnerabilities, and ensuring fixes and patches are implemented in a timely manner.

National Law Review, Volume IX, Number 303

Source URL:https://natlawreview.com/article/could-your-erp-system-make-you-victim-cybercrime