Waterstons
we're with you

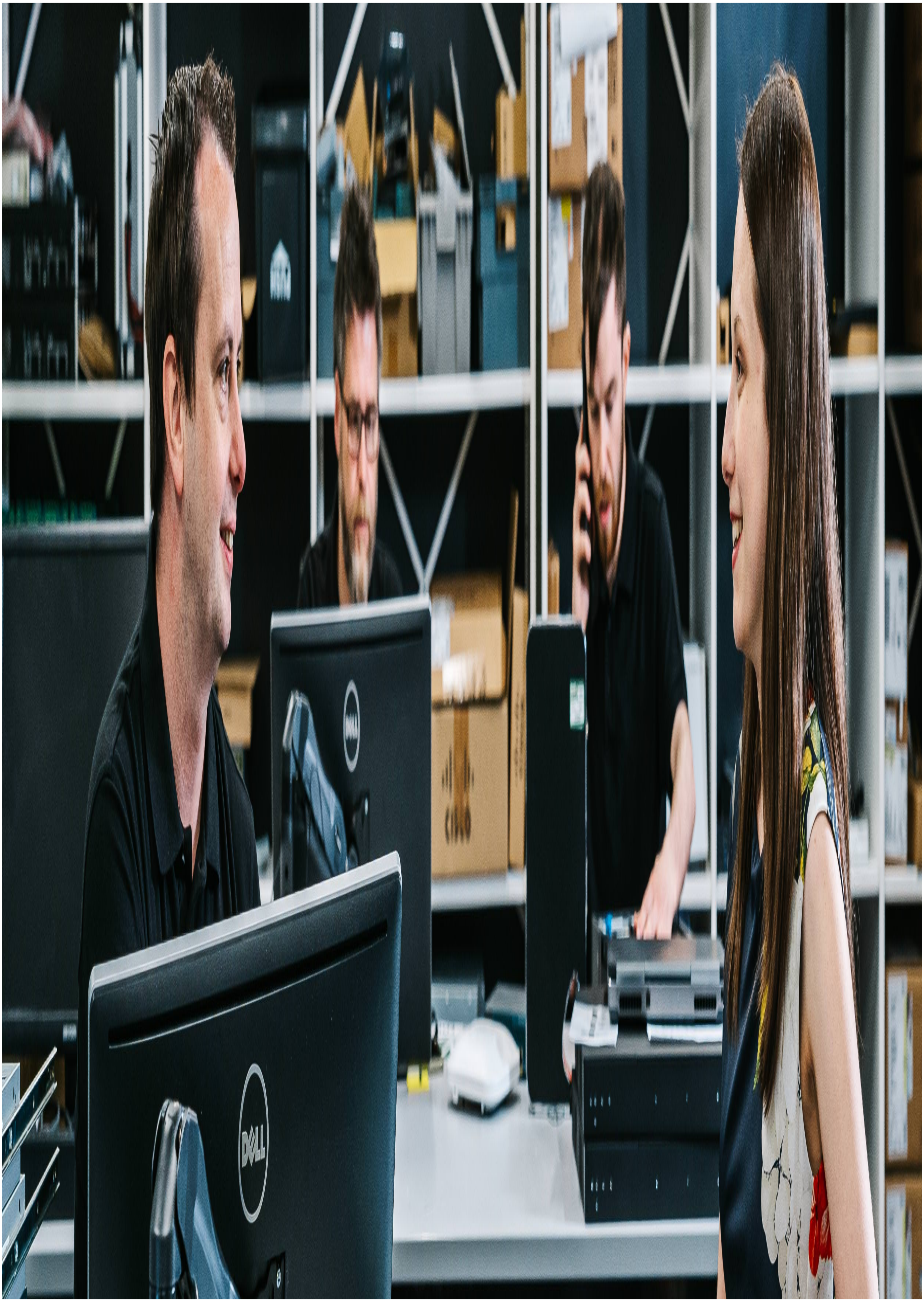
+44 345 094 0945
www.waterstons.com

News article

Dec 2023

Cyber Incident Review

Fidelity National Financial shuts down network in wake of cybersecurity incident.



In late November, Fidelity National Financial (FNF), one of the USA's largest title insurance and settlement services for the mortgage and real estate industries, suffered a significant cyber attack. The attack forced FNF to shut down its IT systems, resulting in real estate transactions being paused.

What happened?

While details of the attack have not been revealed by FNF, the ALPHV/BlackCat ransomware group has claimed responsibility by adding FNF to its leak site - where the group publishes details and stolen information about successful cyber attacks. While this indicates it may have been a ransomware attack, FNF has not confirmed the nature of the attack or if the group were responsible. Neither side has stated if any data was exfiltrated. Following FNF's identification of the attack, the breach was reported to the U.S. Securities and Exchange Commission (SEC), and the organisation's incident response plan was enacted, stating that they had 'blocked access to certain [...] systems, which resulted in disruptions to our business'.

This system shut down impacted both FNF and its subsidiaries, causing real estate transactions to be paused, as well as leading to uncertainty for customers paying mortgages through subsidiaries of FNF. The system's shut down as part of FNF's incident response also included company email services and website, limiting the ability to communicate the issue with customers, and for customers to contact FNF, leading to some confusion and concern over when mortgage and house sale payments would complete.

The primary communication method appears to have been automated voicemail on customer service phone lines, although little detail was available to customers, with the main phone line stating that the company was 'still experiencing a system-wide outage' and that FNF 'did not have access to send or receive email, or access to any system'.

However, this communication was not consistent across all subsidiary companies, with one subsidiary calling the incident a 'catastrophe' in an automated customer support voicemail message. FNF and its subsidiaries have not released any public statements to customers or the media regarding the attack outside of the SEC filings, and their customer support voicemail.

On November 26th, one week after initial disclosure of the breach, FNF announced in a new SEC filing that the attack had been successfully contained and business systems were starting to be restored – although no timeframe. As of December 12th, FNF's website is still unavailable in some regions and no further updates are available on the current status of internal IT systems. On the same day as the recent SEC filing announcing the incident containment, ALPHV/BlackCat removed FNF from the leak site, causing some security researchers to speculate if a ransom demand was paid, although there is no confirmation of this.

The importance of communication in Incident Response

This incident highlights the criticality of an organisation's communication with both customers and business clients/partners during incident response. Despite the importance, communication planning is often overlooked during incident response planning.

Clear communication is key to minimising the reputational impact of an incident and to reassure customers and business partners that the organisation is managing the situation effectively, even more so if the incident results in a prolonged outage or significant disruption.

Organisations should:

• Review their network and begin to classify the security and operational requirements of devices and infrastructure on their network. This should inform how the network is segmented into smaller sections with shared security requirements and controls. A segmented network will allow organisations to take down sections of their network more granularly during the containment phase of incident response to reduce the potential downtime.

• Implement an incident response capability which is regularly tested to provide ongoing confidence in its effectiveness and ensure that all key stakeholders are aware of their responsibilities.

• Ensure that the incident response plan has a well-prepared communications plan to ensure that the organisation, any subsidiaries also impacted, and customers/business partners are kept informed of key incident progress as appropriate. For communications to customers and clients this should outline how frequently updates should be provided and what information should be communicated. Organisations can also prepare pre-approved draft templates for public communications to reduce the time spent drafting and reviewing during the incident response phase.

• Avoid paying ransom demands. There is no guarantee that hackers will decrypt systems or delete stolen data, and it may make the organisation a target for repeat attacks from other threat actors expecting a payout.

This article and other fantastic insights are shared in our monthly cyber threat report. You can join the mailing list to receive it here.

Waterstons has 25+ years' experience across the UK and Australia preparing and protection organisations from cyber threats. We are committed to assisting all organisations to stay agile and prepared in today's cyber conscious economy.

Empower your organisation today, get in touch with one of our team members.