

After a devastating attack by “The Wolf,” Coastline Regional Hospital rebuilds its network security with HP printers and PCs



Official wrap-up report for the data breach on May 22, 2017

Industry
Healthcare

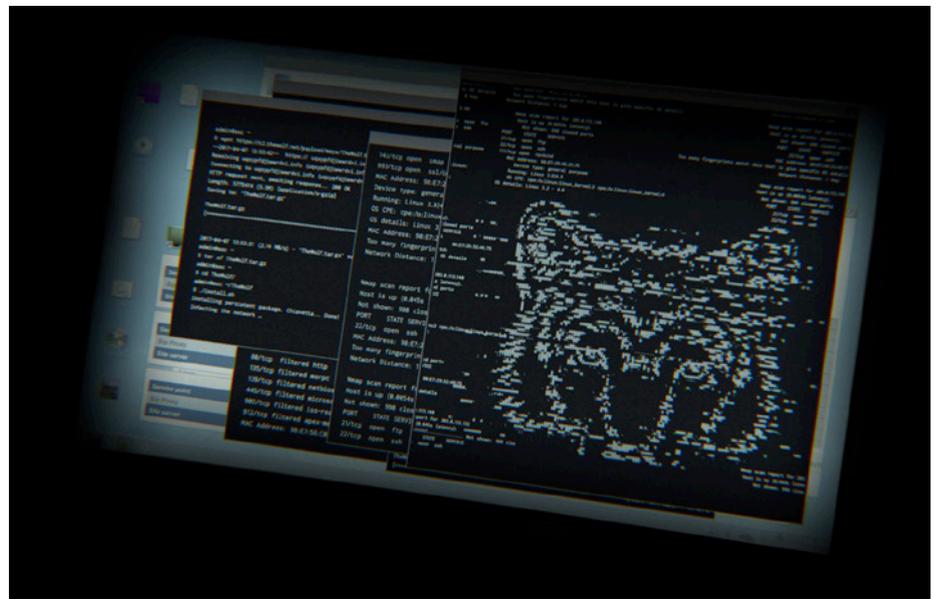
Objective
Address issues that led to breach and update security policies

Approach
Partnered with HP security experts to plan and implement better security practices

IT matters

- Closed security gaps on the network
- Established better security protections and policies to minimise future risks

Business matters
Improved security practices to better protect patient data and regain patient confidence



Overview

Coastline Regional Hospital is a busy regional medical complex, serving hundreds of thousands of patients in its doctors’ offices, emergency clinics, surgery centres, and rehabilitation facilities.

As the hospital has grown, it has become more challenging and time-consuming to keep patient data safe. A few years ago, Coastline outsourced its medical records management to Hoffman Health Technologies, which specialises in digitising, storing, and managing data for many medical centres.

On May 22, 2017, the cyberterrorist known only as “The Wolf” used an unsecured printer at Coastline to infiltrate Hoffman’s network and steal millions of medical records. Following the breach, Coastline Regional Hospital partnered with HP to rebuild and protect its network with HP device, data, and document security.

What happened

Coastline Regional Hospital never saw it coming. They never dreamed an ordinary printer, used every single day, could lead to the theft of millions of medical records. But it was easy for The Wolf to use a simple USB drive to inject malware into a printer. Since the hospital's printer was connected to Hoffman's network, this gave The Wolf access to everything inside both networks, including all that patient data. Both Coastline and Hoffman suddenly found themselves facing millions of dollars in federal and state fines, civil actions, corrective action plans, and lost business from current and future customers.

Why it happened

So, what did Coastline Regional Hospital do to provoke The Wolf? Nothing. It's not anything the hospital did. Rather, it's what it didn't do. Coastline spent a lot of money annually on network security, but it had no security plan for its printers. The Wolf's hack could have been prevented if the printer's USB port had been closed or had required authentication. The malware that was disguised as a software update could have been stopped if the printer had malware protection.

Hoffman Health Technologies failed, too. If it had connected its PCs to network monitoring tools, it would have been notified of the attack immediately. And data stored on its servers would have been unreadable if it was encrypted.

With any of these protections, The Wolf's breach would have been mitigated or stopped, but in their absence, The Wolf succeeded.

Going forward

With HP's guidance, Coastline Regional Hospital replaced and secured its printers and PCs and, in doing so, improved the security of the entire hospital network.

Coastline now has new HP LaserJet Enterprise MFPs and HP Elite PCs with built-in malware protection that can stop an attack and self-heal without IT intervention. HP Access Control and role-based controls let administrators limit access to devices and specific features—like USB ports. The hospital deployed HP JetAdvantage Security Manager for automatic printer hardening and maintenance of security policies. And the HP Manageability Integration Kit (MIK) helped speed up IT management and remotely manage security and software features across the hospital's PC fleet.

Coastline also gave Hoffman the boot, and is outsourcing its medical records management to a new supplier.

Conclusion

Coastline Regional Hospital suffered considerable financial and brand damage due to the breach, the negative publicity it caused, and expensive noncompliance fines. But with a comprehensive security strategy powered by cutting-edge solutions from HP, the hospital's network is more secure than ever. Thanks to HP, Coastline Regional Hospital is ready to rebuild patient confidence and continue with its mission of care.

Coastline Regional Hospital and Hoffman Health Technologies are fictional companies targeted in a large cyberattack in HP's film, "The Wolf: The Hunt Continues."

For more information on HP solutions:

Print security: hp.com/go/reinventsecurity
PC security: hp.com/go/ComputerSecurity

To view "The Wolf" films, visit:

hp.com/thewolf

Sign up for updates
hp.com/go/getupdated



Share with colleagues

