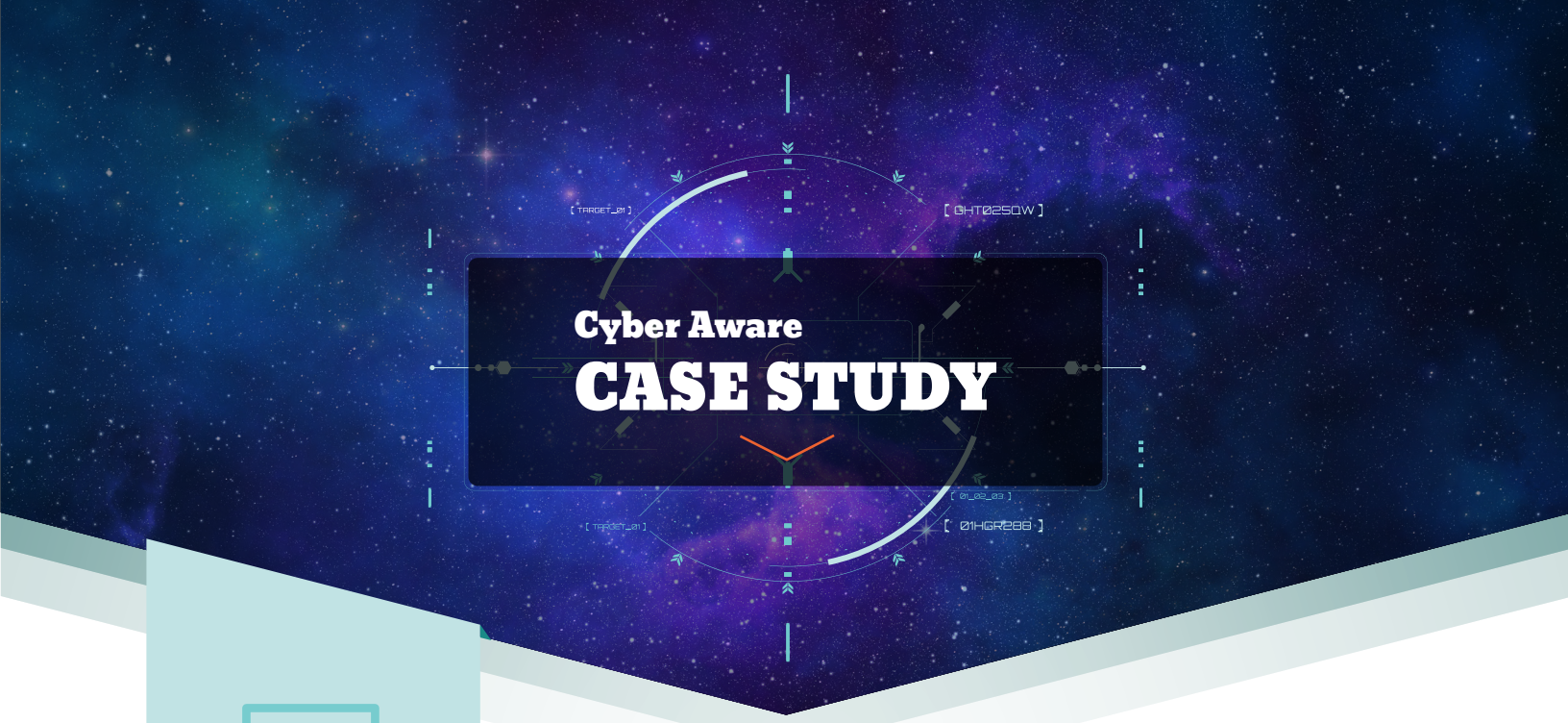

> ...they could have prevented some of the unrestricted access and massive damage the hackers inflicted.

SONY PICTURES ENTERTAINMENT

The Federal Bureau of Investigation attributed the attack on Sony Pictures Entertainment (SPE) to North Korea. This attack erased everything stored on over 3,000 computers and 800 servers, leaked personal documents, records, and embarrassing email to the public and eventually forced SPE to cancel the release of a controversial movie.

A myriad of basic security practices may have provided better protection for SPE networks and files. Had SPE implemented these security practices, it could have prevented some of the unrestricted access and massive damage the hackers inflicted.

Two-factor authentication (2FA) would have provided another layer of protection. 2FA requires both a password and another piece of information, such as a card, fob, or biometric. This added security may not have completely thwarted the hackers, but it would have made it much more difficult. Instead, the hackers used administrative usernames and passwords to gain unfettered access to of SPE's entire network.

Files containing social security numbers and other personal information lacked password protection, and seven years of email messages languished on servers without encryption.

SEPTEMBER 2014

Hackers gained access to SPE by tricking an employee into clicking a malicious email attachment.

Sensitive information, including administrator usernames and passwords, was kept unprotected in spreadsheets and documents, enabling hackers to steal seven sets of administrator passwords. They mapped SPE's entire network, identifying critical files and planning the destruction of servers and computers.

Hackers patiently exfiltrated chunks of data from different servers to multiple hacker-controlled locations, making the theft difficult to detect.

NOVEMBER 2014

A group calling themselves The Guardians of Peace (GOP) locked SPE employees out of their computers and threatened to release sensitive information.

Almost immediately, the hackers leaked unreleased films with other data to follow.

DECEMBER 2014

Hackers released performance reports, medical records, criminal background checks, passport information, salary details, and thousands of embarrassing email messages.

Hackers threatened family members of Sony employees and threatened a 9/11 style attack if SPE released the *The Interview*. North Korea called the film about two journalists recruited by the CIA to assassinate North Korean leader Kim Jong-un an "act of terrorism."

Eventually, *The Interview* was released to 300 theaters on Christmas day. The film was more widely distributed online for rent or purchase through Google Play, Xbox and a special Sony website.

IN CLOSING

State-sponsored cyber criminals present a valid threat, are usually well-funded, and are difficult to defeat, but SPE's lack of security allowed hackers to capitalize on inherent corporate-wide vulnerabilities.