Mind your spreadsheets: Tips to improve your data governance before an incident

May 05, 2022

Even the most secure organizations fall victim to cyber attacks. To be prepared, organizations need to identify and secure or delete certain high-risk forms of data on their systems.

Cyber criminals have been cashing in on organizations' loose information governance practices since the rise of so-called "double extortion" in 2020 in which threat actors encrypt key systems, steal data and demand a ransom in exchange for decryptors and deletion. In this article, we explain how ungoverned data collections can complicate an incident response, and provide helpful tips to improve data management.

Threats

Cyber threat actors now often steal data and hold it for ransom, offering to delete it only after payment of a ransom commensurate with the data's sensitivity.

Although theft of databases does occur, it is common for threat actors to search for and find sensitive files from network file shares. All too often, an organization's file share serves as a digital "junk drawer," storing random files that do not fit squarely into a records retention scheme. This is pay dirt for the threat actor. Sophisticated threat actors will use automated means to harvest loose files from a variety of network locations – endpoints, file shares and e-mail accounts, for example. They will then present unstructured (or "flattened") lists of tens or hundreds of thousands of files back to organizations in an attempt to impede proper valuation and use time pressure to extort a higher payment.

Whether or not the threat actors dump these large caches of data on the dark web, the response can be very arduous because notification to those impacted must usually follow. It is often necessary to send all or most of the data cache for processing e-discovery to identify all the personal information exposed and who it belongs to.

E-discovery has become a major incident response cost, and victimized organizations have a key stake in limiting its scope. The number of affected individuals drives notification and a number of related costs, and is also a key factor in the exposure to

legal claims. Bluntly, an incident with a small group of affected individuals is a much less attractive class action target.

Formal records, scheduled and classified according to their sensitivity, are not the problem. Given they are under governance, formal records tend to be secured appropriately, including by encryption. It is the treatment of file copies, in particular copies of files that are “transitory” or “loose” and ungoverned that tend to cause the size of affected populations to balloon.

Consider the creation of an export file for a project that involves migrating data from one system to another. It contains information about 20,000 individuals, yet is left unencrypted on a file share or on a single employee’s workstation. Files like this – and spreadsheets in particular – build up on a network and can double the population of individuals affected by a network compromise.

What organizations need to do

Organizations must recognize this particular threat and take steps to reduce their ransomware blast radius. In other words, they should assume the data on their networks is at risk of being stolen and take steps to minimize the potential impact of theft.

This can be done through a range of technical means, including through the implementation of segmentation and privilege minimization. Our focus here, however, is on records and information governance, and we make two suggestions:

1. **Organizations should implement a workable policy to govern user behaviour.** Many organizations have implemented clean desk and convenience copy rules to govern physical copies. The rule we contemplate is the electronic equivalent. We say “workable” because any rule that governs the use of sensitive convenience copies has the potential to impede productivity. A good rule will address the risk reasonably, leverage available technology and be acceptable to users.
2. **Organizations should consider conducting periodic network scans.** This means scanning the network to find problem files before a threat actor does. These scans serve the dual purpose of identifying problematic files and ensuring adherence to data policies. There are tools and services available, and like most security solutions, strong implementation is key and no tool is likely to do all the work. With a proper investment and good implementation, however, an organization is likely to eradicate the “low hanging fruit” and mitigate a significant degree of its risk.

Takeaways

Ransomware regularly involves data theft. The threat actor will search for sensitive data wherever it resides. Organizations that have policies and controls to protect their most sensitive data may still have ungoverned loose data on their systems. To avoid a costly e-discovery exercise and unexpectedly large notification obligations, organizations should adopt digital clean desk and convenience copy rules and engage in regular network scanning.

By

Eric S. Charleston, Daniel J. Michaluk

Expertise

Corporate Commercial, Cybersecurity, Privacy & Data Protection

---

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749