Ransomware Relies on Poor Data Access Governance

Protection through Containment In modern building construction, firewalls are put in place to contain the e ects of a fire that might break out in a given area. The idea is that if the fire can be contained to a specific section, then despite the damage, you won't lose the building.

Think of ransomware as a fre that you must be prepared to fght. What can you do to contain ransomware using a similar approach?

Data Access Governance (DAG) is all about controlling insider access to data using concepts such as least privilege and separation of duties. The mention of insider access conjures images of employees doing

Astute security leaders know that the easiest way for outsiders to gain access to their organization's data is through insider access. Compromised credentials and Trojan horses (phishing) are the most common tactics. Data exfiltration (where the bad guys can publish your secrets) and ransomware continue to make headlines. If you don't take precautions against these threats, before you know it, the "building" is on fire. PII, PCI, or PHI. Those file types are definitely important. But ask the CEOs at Colonial Pipeline and JBS Foods what landed them on the evening news? And, in the case of the former, in front of Congress? The lesson is clear: If you don't protect the "crown jewels," you will find yourself poorer, severely wounded, or out of business faster than you can say, "It won't happen to me." It will happen to you and it's only a matter of time. Based on the principles of well-known security frameworks such as Gartner's CARTA and the

- Can you verify that the files you consider the "crown jewels" of your organization are stored in locations with restricted access permissions?
- What would happen if these files were compromised through ransomware?
- Can you easily conduct a leastprivilege analysis of employee access permissions?
- Are you conducting regular access reviews?

Identifying What Needs Protecting Which files need the most protection? Sure, you can get in trouble by not adequately protecting compliance-related data such as but it's no silver bullet. For example, many times the ransomware attack vector involves the employee's own machine, which holds the decryption keys for seamless day-to-day access. Furthermore, even if you happen to be attacked in a way other than through the machine that holds the keys, data encryption really only helps with the threat of exfiltration. It doesn't keep the bad guys from locking you out of your own data.

Even though there are no silver bullets, there is an arsenal. Along with the usual measures of user education and patching, we really need to talk about DAG (and related technology such as NetIQ Privileged Access Management (PAM) by OpenText for correcting the real problem of over exposure. Use of these technologies can significantly mitigate As you move forward, you'll have a "building" with a data footprint like this:





