HOW GRC CAN HELP YOU STAY A STEP AHEAD OF RANSOMWARE
FOR LESS RANSOMWARE RISK AND GREATER OPERATIONAL EFFICIENCY, THINK GRC.

It was a one-two punch that many government agencies and other organizations didn't see coming: First, the WannaCry ransomware attack struck in May 2017 and then, just weeks later, came the June 2017 Petya attack. Both affected public-sector organizations worldwide, notably including the United Kingdom's National Health Service (WannaCry) and government-run banks and other offices in Ukraine (Petya). In the United States, WannaCry affected some federal government agencies and also made appearances at the state and local levels, including in Connecticut’s state court system and in local Cook County government offices in the Chicago area. Meanwhile, the private sector was hardly immune: WannaCry affected Nissan and Renault automotive plants, among other businesses, and Petya disrupted operations at WPP, the world's largest advertising agency.

WannaCry and Petya are stark reminders to all organizations—federal agencies, state and local governments, and private-sector businesses—of the danger that cyber attacks pose. Many of these entities are now laser-focused on the question of how to better prepare for, as well as respond to, the next attack. With ransomware growing at 350% annually,¹ there will no doubt be a next one.

There’s more to coping with ransomware, though, than responding in a panic to the appearance of a threat or to a full-blown security incident. Every attack brings a renewed emphasis on reporting on status and impact. And all organizations have steps to take in preparation for an eventual attack that will not only limit the risk of damage, but create opportunities for optimized IT operations over the long term.

While long-term operational improvements may not be top of mind for a government IT security team charged with cybersecurity, they’re worth thinking about in the context of a cyber attack, as this paper will illustrate. Governance, risk and compliance (GRC) is often not the first area of IT that comes to mind in the context of cybersecurity, but there’s an important role GRC solutions can play in helping organizations prepare for and respond to the next ransomware assault on IT systems.

THE GRC-CYBERSECURITY CONNECTION

GRC solutions that help manage risk and compliance are vast repositories of IT systems information. That data exists in an organization’s GRC systems to document and demonstrate compliance—but it’s also precisely the kind of data that can be invaluable for addressing many organizational risks, including ransomware risk.

GRC use cases such as assessment and authorization (A&A) serve as systems of record for hardware, software and information assets. They are designed primarily to document assets for purposes of certification and accreditation, and are also useful in a variety of other areas, including risk management, incident management and business resiliency. But it’s important to be aware that the information used for these purposes can be extremely valuable to cybersecurity teams who need to be able to ascertain what assets would be at risk when a threat is detected or a ransomware attack occurs.

The key is being able to understand what vulnerabilities the ransomware threat is exploiting, quickly run a report from the GRC solution and then take decisive action to address systems that are likely to be impacted. To do these things, you need capabilities that integrate data from internal, third-party and other systems across multiple use cases and workflows. These capabilities facilitate organizational connections across data and processes for use in a variety of different contexts, including ransomware detection and response.

**HOW GRC DATA HELPS ORGANIZATIONS HANDLE CYBERSECURITY PROACTIVELY**

Leveraging GRC data to understand what hardware systems and software applications serve the organization and where they (and their users and admins) are located is fundamental to keeping technology from being unduly impacted by a ransomware attack. That information can, for example, play an important role in developing a strategic and rapid remediation patching program to prevent critical systems from being damaged as a result of a known vulnerability ransomware actors could exploit. Knowing the purpose and location of systems and information makes it possible to determine their relative criticality within your GRC solution—and that, in turn, makes it possible to prioritize actions.

Prioritization is essential to any remediation program, given the growing number of threats and vulnerabilities and the need to test patches prior to implementing them. There is simply no practical way to test every patch or to patch every vulnerability in a timely way. We saw this in play during WannaCry, when it turned out Microsoft had issued a patch months before the attack, but many organizations failed to implement it in time to protect vulnerable systems.² This is why system documentation is key—it’s what reveals, for example, whether a server contains vital source code or just a cafeteria menu, so that priorities can be set accordingly and patches applied in time to have an effect.

Some public-sector organizations were better prepared for WannaCry than others in that their GRC solution allowed them to quickly run a report, understand which systems weren’t properly patched to mitigate the risk of

---

bad actors exploiting a known vulnerability, and leverage notifications and workflows to drive immediate action to protect the organization.

This exploration of how to use GRC data proactively to protect systems from ransomware attacks raises another important point about cybersecurity today: It’s not just the threat detection team that benefits from GRC documentation as a cybersecurity tool. It’s the desktop team, the network team, the people responsible for data backup, business resiliency and other relevant areas—essentially, everyone who has an interest in the well-being of systems in the organization. As one state government director of risk and compliance commented to RSA, “The cybersecurity team is not the only one responsible,” adding that “every person has to think about security in everything they do now, because breaches can happen at the lowest tactical levels. Getting systems information to all the teams is critical.”

**HOW GRC DATA HELPS ORGANIZATIONS RESPOND TO AN ATTACK**

GRC solutions traditionally allow organizations to put controls in place that will help significantly reduce the risk of a ransomware attack. The potential for organizations to be adversely impacted by ransomware and other types of attacks illustrates the need for a strong GRC program and for controls that are firmly in place and tested frequently. In addition, one of the worst consequences of not being fully prepared for a cyber attack is not being able to pinpoint where a ransomware attack is happening and how damaging its potential impact could be—and also not being able to quickly and accurately report that status to senior leadership.
The same GRC data used to determine the risk profile and criticality of systems, and to support a strategic patching program, can also aid in threat detection and response by providing detection and response teams with the visibility they need to respond accurately and confidently. To return to the example in the preceding section, if a threat response team can determine that one group of servers under attack contains information assets vital to the organization’s ability to operate, while another server hosts relatively inconsequential assets, that provides the context needed to prioritize the response. Government organizations, especially at the local level, are likely to be operating with limited resources and staff, forcing them to make “what do we do first?” decisions on a regular basis. For this reason, the ability to set response priorities strategically could make the difference between a catastrophic shutdown and a minor inconvenience.

Part of the challenge of providing GRC information to the people who need it is that often in government, groups and teams that manage different processes aren’t connected with each other, and the processes themselves aren’t connected with the relevant tools. For example, an A&A solution may not directly interface with the organization’s security incident response tool, or information may not be mapped between applications and the systems on which they run. In order to manifest situational awareness to enable and enhance a coordinated response to ransomware, government organizations may need to rethink how they structure information sharing, aided by solutions that are expressly intended to connect with other systems and the people who use them.

As one state government director of risk and compliance mentioned previously told us, “We have GRC information centrally available to server admins and threat detection teams, among others. That’s how we see where exactly a ransomware attack could be occurring.”
IT’S NOT JUST ABOUT ADDRESSING THREATS—IT’S ABOUT OPTIMIZING OPERATIONS

The integrated, connected approach to ransomware that makes it possible to prepare for and respond to threats more effectively also enables organizations to operate more efficiently and productively. Given the budget constraints within which public-sector organizations often operate, the ability to identify and prioritize threats and targets quickly is essential to enabling a small team to accomplish more with fewer resources than a private company is likely to have. In addition, organizations enjoy a greater return on their investment in a GRC solution when they can also leverage it to react to a ransomware threat and diminish the impact.

A recent Forbes Insights report posed an interesting question: “Is risk management a means to avoid losses or a tool for creating value around optimizing outcomes?” In light of the opportunities GRC can create across the organization, that’s not really an either-or question, but one that can be answered with a resounding “Yes!” And while the question was raised mainly in the context of the private sector, it rings true for government too. IT teams in government organizations large and small can help limit their organizations’ ransomware risk by addressing the possibility of attack through the use of GRC-enabled preventive measures and by prioritizing information to be shared across systems, assets, admins and users. In the process, they create rich opportunities for more efficient, effective operations.

ABOUT RSA

RSA offers Business-Driven Security™ solutions that uniquely link business context with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90% of the Fortune 500 companies thrive in an uncertain, high-risk world. For more information, go to rsa.com. Learn about RSA Archer® solutions for GRC, including RSA Archer Assessment & Authorization, at rsa.com/archer.

3Hugo Moreno, “Are You Missing The Opportunity In Risk?” Forbes Insights, May 24, 2017

RSA and the RSA logo are registered trademarks or trademarks of Dell Technologies in the United States and other countries. © Copyright 2017 Dell Technologies. All rights reserved. Published in the USA. 10/17. White Paper, H16605

RSA believes the information in this document is accurate as of its publication date. The information is subject to change without notice.