Seize Control of Your Cybersecurity

SAI360

Organizations today are juggling risks related to compliance, environmental issues, third parties, and more. For companies in all industries, digital risk is one of the most challenging to address.

Ransomware, has become a significant concern in recent years, with increasing frequency. For example, in May 2017 the WannaCry attack affected companies worldwide and dramatically increased the visibility of ransomware among corporate leaders. Experts suggest that losses from the WannaCry incident could reach $4 billion USD[1].

Through comprehensive digital risk management, your company can position itself to achieve business excellence, support growth, and create trust among customers and other key stakeholders. One important component of this approach is leveraging the controls that you already have in place, such as ISO/IEC 27002:2013 Information technology—Security techniques—Code of practice for information security controls.

Implementing policy-based ransomware risk mitigation

When it comes to ransomware[2,3], an essential first step is conducting discovery and assessing the dangers. The next step is developing policies, procedures, and controls that align the organization and provide a consistent approach for responding to ransomware threats. Once policies and controls have been implemented, organizations can begin the ongoing process of training employees, monitoring performance, and improving policies and procedures continually over time.

Standards play a central role as organizations create programs to address ransomware risks.

- ISO/IEC 27002 is a useful framework that outlines best practices related to information security controls.
- ISO 27002 is used by organizations that hope to achieve ISO 27001 certification, as well as by organizations that simply want to develop their own information security management guidelines based on commonly accepted controls.

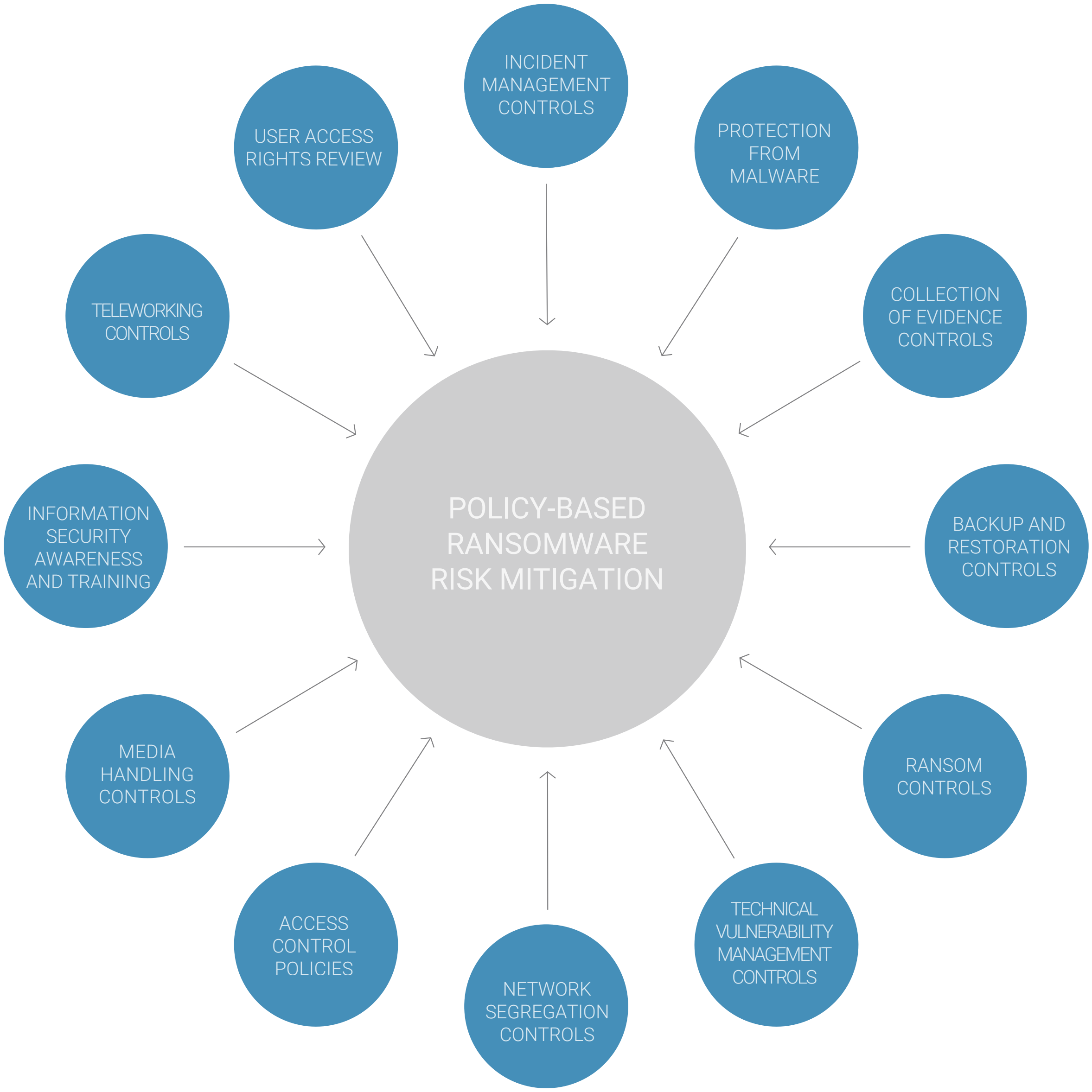
[1] Sherr, I., 2017, "WannaCry ransomeware: Everything you need to know", CNET.com, May 19, 2017, cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses

[2] For a more detailed explanation, see, "GB 206-2017: Surviving ransomware: A best practice guide for enterprises (ISO 27002)"

[3] Schaffhauser, D., 2015, "MIT Formally Kicks Off Cybersecurity Work", CampusTechnology.com, March 16, 2015, campustechnology.com/articles/2015/03/16/mit-formally-kicks-off-cybersecurity-work.aspx

SAI GLOBAL

FIGURE 1. ISO27002 CONTROLS FOR POLICY-BASED RANSOMEWARE RISK MITIGATION


INCIDENT MANAGEMENT CONTROLS
PROTECTION FROM MALWARE
COLLECTION OF EVIDENCE CONTROLS
BACKUP AND RESTORATION CONTROLS
RANSOM CONTROLS
TECHNICAL VULNERABILITY MANAGEMENT CONTROLS
NETWORK SEGREGATION CONTROLS
ACCESS CONTROL POLICIES
MEDIA HANDLING CONTROLS
INFORMATION SECURITY AWARENESS AND TRAINING
TELEWORKING CONTROLS
USER ACCESS RIGHTS REVIEW
POLICY-BASED RANSOMWARE RISK MITIGATION

Managing employee work practices

Experience suggests that as many as 70% to 80% of cybersecurity breaches[4] are caused by employee actions, such as clicking on a malware link in an email or on a website.As a result, one focus area in ISO 27002 are controls related to employee work practices.

These include:

TELEWORKING CONTROLS

Since teleworking is commonplace today, ransomware controls are necessary to protect data, equipment, and networks when employees are offsite. These include controls to protect files, as well as backup and recovery capabilities.

INFORMATION SECURITY AWARENESS AND TRAINING

Educating employees about how their actions affect security can prevent ransomware attacks. It is crucial that employers understand and implement company policies that can help reduce ransomware threats to front-line employees. Behavioral and technical measures used hand in hand are an effective way to address digital risks, such as ransomware.

MEDIA HANDLING CONTROLS

These measures dictate how storage media like thumb drives and external hard drives should be handled to protect them from ransomware attacks. Savvy media handling controls should also outline procedures for restoring data from removable media.

[4] Schaffhauser, D., 2015, "MIT Formally Kicks Off Cybersecurity Work", CampusTechnology.com, March 16, 2015, campustechnology.com/articles/2015/03/16/mit-formally-kicks-off-cybersecurity-work.aspx

Limiting user access

Files with sensitive and valuable information are the holy grail for cybercriminals. Limiting user access to information can minimize the negative impact of a ransomware attack. Accordingly, ISO 27002 recommends implementing policies related to access control, as well as periodic reviews of user access rights.

ACCESS CONTROL POLICIES

These controls define which employees have access to different types of information. Often access controls are configured based on employee roles.

USER ACCESS RIGHTS REVIEW

Organizations should review the access requirements that end users have to different types of information. As a general rule, privileged access should not be widely granted, and it should be reviewed periodically, as employees join and depart the company, as well as when staff change roles and levels.

NETWORK SEGREGATION CONTROLS

It is possible to limit user access to networks based on frameworks related to trust levels, organizational structure, or other factors. As with other controls, the goal is to minimize the reach of a ransomware attack, should one occur.

Technical solutions

ISO 27002 recommended technical controls for combating ransomware may be proactive or reactive in nature. For example, antivirus and malware solutions attempt to stop ransomware attacks before they start. Similarly, IT teams should proactively search for system vulnerabilities and remedy them. If an attack does occur, backup and restore controls can minimize the damage.

PROTECTION FROM MALWARE

These controls work by preventing unlimited user access to software, websites, and services. Another key component of malware protection is developing and executing policies related to updating software, antivirus and malware solutions, and operating systems. Many cybercriminals intentionally target systems that are out of date.

TECHNICAL VULNERABILITY MANAGEMENT CONTROLS

The goal of these controls is to seek out system vulnerabilities and then take appropriate action. Responses include system updates or minimizing user access to systems that are less robust than desired.

BACKUP AND RESTORATION CONTROLS

It is essential for organizations to have policies related to data backup and recovery. In addition, these processes must be periodically tested to ensure that they are effective. Backup and restore are among the most effective defenses to a ransomware attack.

Responding when (not if) an attack occurs

While organizations always strive to avoid security breaches, incidents like ransomware attacks still occur. To minimize the chaos when reacting to these crises, ISO 27002 goes so far as to prescribe controls related to the organizational response and evidence collection. Your organization should also establish protocols for communicating with criminals.

The ransomware landscape today

Ransomware perpetrators are continually developing new approaches to capitalize on stolen information. Ransomware specifically, and digital risk in general, are moving targets. As a result, organizations must implement flexible and dynamic risk management programs. Companies need to constantly monitor the risk landscape and adjust their policies and controls as circumstances change. Recent trends in ransomware include:

Ransom demands come in many varieties. Some cybercriminals have implemented a sliding scale where ransom fees increase over time. Others have even offered to release files for free, if the victims agree to infect others with the ransomware.

Ransomware is becoming more targeted. Research suggests that phishing is a growing source for ransomware attacks. McAfee reported that social engineering and phishing attacks represented 21% of ransomware incidents to date in 2017, compared to just 8% in 2016.

Cybersecurity insurance is one possible response. PricewaterhouseCoopers recently estimated that in 2020, companies will spend $7.5 billion on cybersecurity insurance, compared to $2.5 billion in 2015.

Companies are taking a more proactive stance. One example is the collaborative called Nomoreransom.org. Security vendors, law enforcement agencies, hosting companies, insurance companies, and others have joined forces to combat ransomware. The group has developed 27 free decryption tools that can be used to recover captive information.

Sources:
Verizon’s 2017 Data Breach Investigations Report www.verizonenterprise.com/verizon-insights-lab/dbir/2017
Get Hacked and Your Cybersecurity Company May Pay www.technologyreview.com/s/608160/get-hacked-and-your-cybersecurity-company-may-pay

INFORMATION SECURITY INCIDENT MANAGEMENT CONTROLS

When defining how your organization will respond to a ransomware attack, key considerations include assignment of employee responsibilities and reporting requirements.

INCIDENT MANAGEMENT COLLECTION OF EVIDENCE CONTROLS

Organizations must be prepared to collect digital forensic evidence if an attack occurs. The process for gathering this evidence needs to be defined well before an attack occurs. For example, relevant information may be contained in email logs, firewall and network logs, and Bitcoin wallet addresses.

COMMUNICATION WITH CRIMINALS AND RANSOM CONTROLS

Although this issue is not outlined explicitly as a control area within ISO 27002, organizations should establish guidelines for any communication with cybercriminals regarding ransom payments or other data extortion issues. Ideally, only certain designated employees should be empowered to communicate with cybercriminals. In addition, messages should be consistent with the organization's business goals and policy controls.

Next steps: Defending the enterprise

When it comes to ransomware risks, risk management activities are only as effective as the information backing them. The first steps in the risk lifecycle framework are to better understand the hazards associated with ransomware and then develop policies to address them. Knowledge is power, but understanding where to begin can be daunting. SAI Global's domain experts have developed world-class standards and content designed to help organizations anticipate, interpret, and optimize digital risks.

To learn more about how to understand, prepare, and defend your enterprise from ransomware threats, download the best practice guide, Surviving Ransomware[5] or download ISO/IEC 27001:2013[6] (detailing requirements for establishing, implementing, maintaining and continually improving an organization's information security management system).

[5] See "GB 206-2017: Surviving ransomware: A best practice guide for enterprises (ISO 27002)" ; infostore.saiglobal.com/en-us/Standards/GB-206-2017-1925020

[6] See "ISO/IEC 27001:2013"; infostore.saiglobal.com/en-us/Standards/ISO-IEC-27001-2013-1677321/

About SAI Global

SAI Global helps organizations proactively manage risk to create trust and achieve business excellence, growth, and sustainability. Our integrated risk management solutions are a combination of leading capabilities, services and advisory offerings that operate across the entire risk lifecycle allowing businesses to focus elsewhere. Together, these tools and knowledge enable clients to develop an integrated view of risk. To see our tools in action, request a free demo.

We have global reach with locations across Europe, the Middle East, Africa, the Americas, Asia and the Pacific.
For more information visit www.saiglobal.com.

SAI GLOBAL