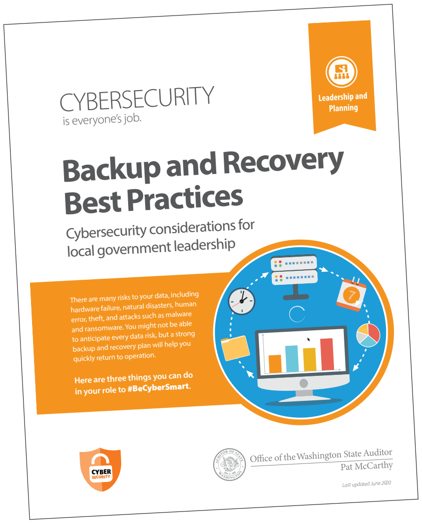
PERFORMANCE AUDIT

Report Highlights

Office of the Washington State Auditor
Pat McCarthy

Data Backup and Disaster Recovery



CYBERSECURITY
is everyone's job.

Leadership and Planning

Backup and Recovery Best Practices

Cybersecurity considerations for local government leadership

There are many risks to your data, including hardware failure, natural disasters, human error, theft, and attacks such as malware and ransomware. You might not be able to anticipate every data risk, but a strong backup and recovery plan will help you quickly return to operation.

Here are three things you can do in your role to #BeCyberSmart.

CYBER SECURITY

Office of the Washington State Auditor
Pat McCarthy

Last updated June 2020

Learn about actions local governments and others can take to improve backup and recovery practices in this booklet of resources developed by our Office.

Washington state agencies are required to keep their data and information technology (IT) systems safe from a variety of events including network outages, security incidents, and natural disasters. Being unprepared for these events can lead to a disruption of critical state services, lost revenue and records, and reduced organizational effectiveness.

This audit looked at two areas: data and system backup and disaster recovery. A backup is simply a copy of your data or system. A disaster recovery plan sets out, in policies and procedures, how you will recover data and restore full system operations to ensure business continuity. Earlier audits performed by our Office found agencies usually had data backup procedures, but did not consistently perform tests to verify they could restore critical data. Furthermore, even fewer had a current and tested disaster recovery plan.

Audited agencies can improve their ability to restore critical systems and data in the event of a disaster or security incident

This audit evaluated whether four state agencies had proper backup strategies and disaster recovery procedures in place, including testing the plan, for selected systems. We compared our observations to state requirements and leading practices.

We found none of the four audited agencies fully and consistently met all state requirements for data backup, disaster recovery, and testing recovery plans. In addition to meeting state requirements, agencies could further reduce disruptions to their services and operations by following the backup and disaster recovery guidance offered by leading practices.

Report number 1026917, published 9/17/2020, online at www.sao.wa.gov

Audited agencies lacked the resources and guidance they needed to establish comprehensive backup and disaster recovery practices and procedures

Executive management at some agencies were not always aware of all risks and potential consequences, and so did not always allocate adequate resources to address the risks. We found none of the four audited agencies adequately used IT risk assessments and business impact analyses to identify and inform management of the risks. Executive management's investment in technology and staff is nonetheless key to implementing effective backup strategies and disaster recovery plans. Better statewide guidance and tools could help agencies implement more effective backup strategies and disaster recovery plans.

State Auditor's Conclusion

State agencies' ability to provide essential services relies heavily on the availability of a variety of IT systems. Any number of things can happen to interrupt the availability of those systems, including relatively mundane equipment failures, unforeseen natural disasters, or malicious security attacks. When these events happen, it is important for agencies to have reliable backups of their systems and their data, as well as a solid plan to recover their most important systems quickly.

The state's security requirements and other sources of leading practices can help agencies develop effective backup and disaster recovery plans that are tailored to the business needs and risks each agency faces. In the appendices of this report, we have compiled those requirements and leading practices in one place. These are important resources, and we would encourage all state agencies to take advantage of them as they develop their own recovery plans.

Recommendations

We gave detailed recommendations to the four agencies that addressed three issues:

- Using IT risk assessments and business impact analyses to identify gaps in current backup and disaster recovery practices and procedures
- Ensuring management is aware of issues affecting data backup and disaster recovery efforts, so they can adequately address them
- Implementing backup and disaster recovery procedures and processes that align with state requirements and leading practices

We further recommended the Office of the Chief Information Officer help agencies develop more effective and comprehensive backup and disaster recovery processes by providing clear and up-to-date guidance.

Government organizations could also refer to the #BeCyberSmart section of the State Auditor's Office website for additional resources. It contains a set of curated resources our Office has compiled on various cybersecurity issues. Though these resources are intended to assist local governments with cybersecurity, state agencies may also find some of them helpful, in particular the Backup and Recovery Best Practices brochure.

Leadership and Planning

You have an important role to play

As a leader, you help set the tone and cultural direction of your organization. By starting with these three steps, and ensuring the departments within your government work together on these issues, you are on your way to improving your cybersecurity program.

Department of Homeland Security - Questions every CEO should ask about cyber risks:
https://www.us-cert.gov/ncas/tips/ST18-007

Our Office also offers training at conferences on cybersecurity. For upcoming dates and times, visit

sao.wa.gov/BeCyberSmart

Sources:
Department of Homeland Security
National Institute of Standards and Technology
Center for Internet Security

Center for Government Innovation