



White Paper

TESTED, NOT JUST WRITTEN

Ransomware Readiness Lessons from the Field

TESTED, NOT JUST WRITTEN

Ransomware Readiness Lessons from the Field

CONTENTS

The plan is not the capability	03
Four assumptions every plan makes until it is tested	06
Two ways to find your gaps before an incident does	12
Case study: real-world ransomware response and recovery	13
What this engagement shows every organization that hasn't been tested yet	14
Why this matters to the people who answer for it	16
Next steps	19
About Securance	21
Sources	22

1. The plan is not the capability

When auditors go looking for disaster recovery and incident response plans, they usually find them. What they find less often is evidence that anyone has tested one.



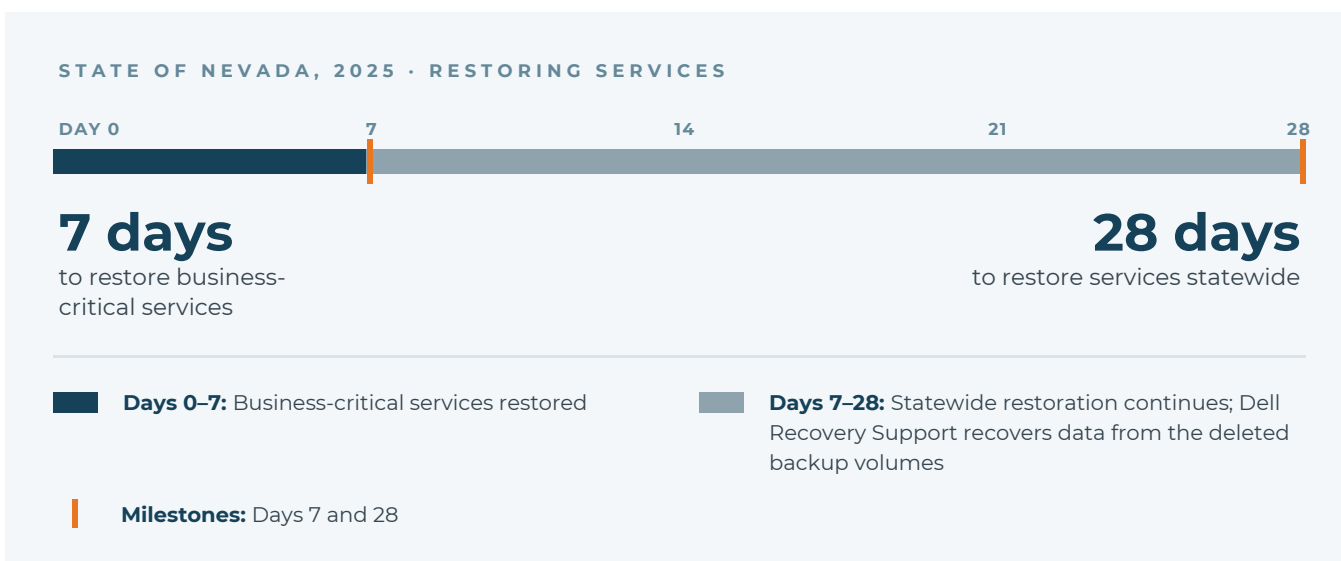
In July 2024, Michigan's state agencies had approximately 370 disaster recovery plans on file in the system the state uses to manage them. When the Auditor General reported on those plans in August 2025, the first finding was that they might not be updated or tested annually, because the dashboard used to monitor them didn't track when each plan was last updated or when its next test was due.¹ The state could show that the plans existed, but not that anyone had tested them.

For a long time, that would have been a tolerable gap, because recovery was a technical problem with a technical answer. Keep good backups, keep them current, and the worst case would be an expensive week of recovering systems and data from them. An untested plan was a risk of inefficiency more than a risk of failure.

The gap stopped being tolerable once ransomware operators started going after the means of recovery before encrypting anything: the backups, the virtualization layer that production runs on, and the credentials that control both. In August 2026, the FBI, CISA, and four partner agencies published a joint advisory on the Gunra ransomware group. Against one victim, the advisory says, the actors deleted the backups and archived data at both the primary data center and the disaster recovery center, before the ransomware ran and again after.² Nevada's statewide incident a year earlier ran in the same order. The attacker moved between critical servers, including the password vault server, retrieving passwords for 26 accounts, then authenticated to the backup server and deleted the backup volumes. Only after that did the attacker deploy the ransomware onto the virtualization servers.³

This means a plan can be technically sound, recently reviewed, and still non-executable, because it names tools that will not be there when someone opens it. The annual review won't catch that. A review checks the plan against itself and determines whether it is complete, current, and approved. Only exercising the plan checks it against the conditions it will face.

The Nevada incident shows what losing the recovery path costs, even in a response that went well by most measures. The state restored business-critical services within seven days, refused to pay the ransom, and published a detailed after-action report.^{3,4} But with its backup volumes deleted, the state engaged Dell Recovery Support to recover the data, and that work lasted the full 28-day recovery.³

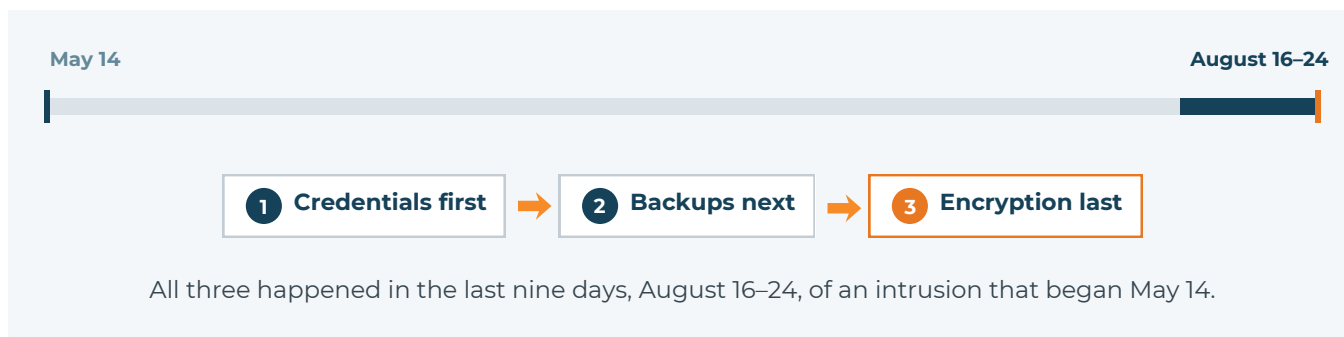
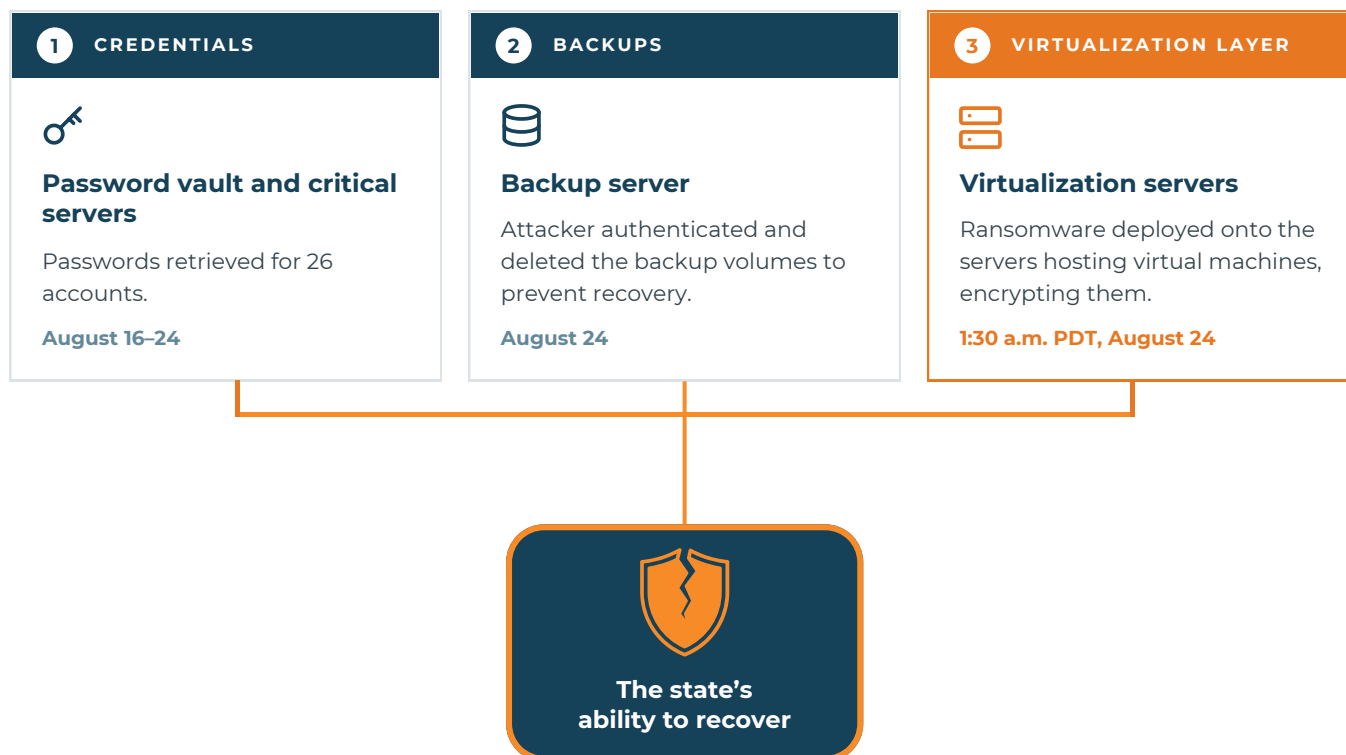


An incident response plan rests on assumptions about the environment, the people, and who has the authority to make decisions once an incident starts. Those assumptions will get tested. The question is whether you run the test, or an attacker does.

What follows is four of those assumptions, one real ransomware engagement in which three of them were tested during the response, and what all of it changes for the people responsible for readiness.

FIGURE 1: RECOVERY UNDER ATTACK

What Nevada's attacker did to the means of recovery



2. Four assumptions every plan makes until it is tested

Every plan rests on assumptions nobody wrote down, because nobody thought to question them. In a ransomware incident, four of them carry most of the weight.

FIGURE 2: FOUR ASSUMPTIONS, FOUR TESTS

ASSUMPTION	WHAT HAPPENS WHEN IT'S WRONG	THE TEST THAT SURFACES IT
The plan will still be executable. The tools it names will be there when it is opened.	The response opens with a plan that references a backup console, an identity provider, or a contact list the attacker has already taken away.	A restoration test: whether systems can be restored from backup, how long it takes, and what the team does when the console is gone.
Someone can make the call. Authority exists before the hour when it is needed.	Hours go to working out who decides, spread across dozens of small delays nobody logs afterward.	A tabletop exercise with the named people in the room. No technical staff standing in for executives.
The signal will be recognized. Detecting something and understanding it are the same act.	A tool quarantines the threat and the alert closes. What the threat already set up stays in place, and the network comes down weeks later.	A look back at closed alerts, and a timed simulation: what the monitoring sees, who reviews it, and what happens to an alert once a tool reports it handled.
Recovery time is restoration time. Returning the data returns the organization.	The recovery objective is met on paper while the organization stays down through rebuilds, revalidation, and reconnection.	A timed end-to-end recovery of one critical system, measured to the point of safe production use, not to the end of the copy.

2.1 That the plan will still be executable

Read an incident response plan closely and it names things: a backup console, an identity provider, a virtualization manager, and a contact list that lives on the network the plan exists to protect. Every one of those names carries an assumption: that each will survive the event the plan was developed for.

The Gunra and Nevada attacks were built to break that assumption. The Gunra actors didn't stop at the primary site's backups. They deleted the disaster recovery center's too, both before and after the ransomware ran. Doing it twice is what an operator does to remove the option of not paying. In what the advisory describes as a traditional double-extortion model, deleting backups isn't Gunra's only lever. The actors exfiltrate sensitive data before encryption and, if the ransom isn't paid, threaten to publish it on their leak site. An organization that restores its systems cleanly still has that threat to answer. The advisory also describes the actors deleting volume shadow copies before encryption and extracting password hashes from compromised domain controllers.² An organization working its plan after an attack like that opens the backup console and finds nothing behind it, and the accounts it would use to rebuild its infrastructure are already in someone else's hands.

The contact list is exposed the same way. Phone trees, escalation contacts, and vendor numbers often live on the file share or in the email system, inside the blast radius, and an organization that has never tried to work its plan from outside its own network tends to find out during the incident that it can't.

A restoration test answers three questions the plan cannot: whether systems can be restored from backup, how long that takes, and what the team does when the console is gone. The test doesn't have to cover the whole environment to be worth running. One critical system, restored end to end and timed, will tell an organization more about its recovery position than another cycle of reading the document.

2.2 That someone can make the call

Plans are written in the passive voice. Systems are isolated. Stakeholders are notified. A decision is made. An incident demands the active-voice version of every one of those sentences — at three in the morning. Isolating a system means taking a service away from the people who depend on it, which is a decision somebody has to own in front of a manager, a regulator, or a resident. A plan that doesn't name that person leaves the question of who decides for the middle of the incident, when every hour spent answering it is an hour the attacker still has access.

Plans are written in the passive voice. An incident demands active voice.

Decision rights are not the same thing as an org chart. The org chart says who reports to whom. Decision rights say who can disconnect a network segment, notify a regulator, or tell the public that a service is down, without first asking anyone. Each of those is hard to take back. Most plans document the org chart and assume the decision rights.

Nevada is the instructive case here, because its response went well. The state escalated the first sign of the outage to its chief information officer and the governor's office in under six hours, and from then on the governor's office set and reaffirmed restoration priorities every day.³ The after-action report credits the response to years of planning and annual incident response simulations "conducted across multiple agencies and leadership levels."³ When the Governor's Technology Office briefed the state's Commission on Homeland Security in February 2026, it described leadership coordination during the response as "rapid escalation and clear decision lanes" between the agencies involved. Among the changes that followed, the same briefing listed "governance and policy improvements: clarify decision rights, strengthen standards."⁵

The briefing doesn't say which decisions needed clarifying. The after-action report offers one clue, at the agency level: "application ownership is an issue and requires additional process improvements and regular review."³ Still, the pairing of "clear decision lanes" with "clarify decision rights" shows something plans tend to miss. Lanes can be clear at the level of who leads the response while decisions inside those lanes are still unassigned, and it takes an incident or a rehearsal to find out which ones. A rehearsal only finds them if the people named in the plan are the ones deciding, in a room, against a clock, with the information they would have on the night.

2.3 That the signal will be recognized

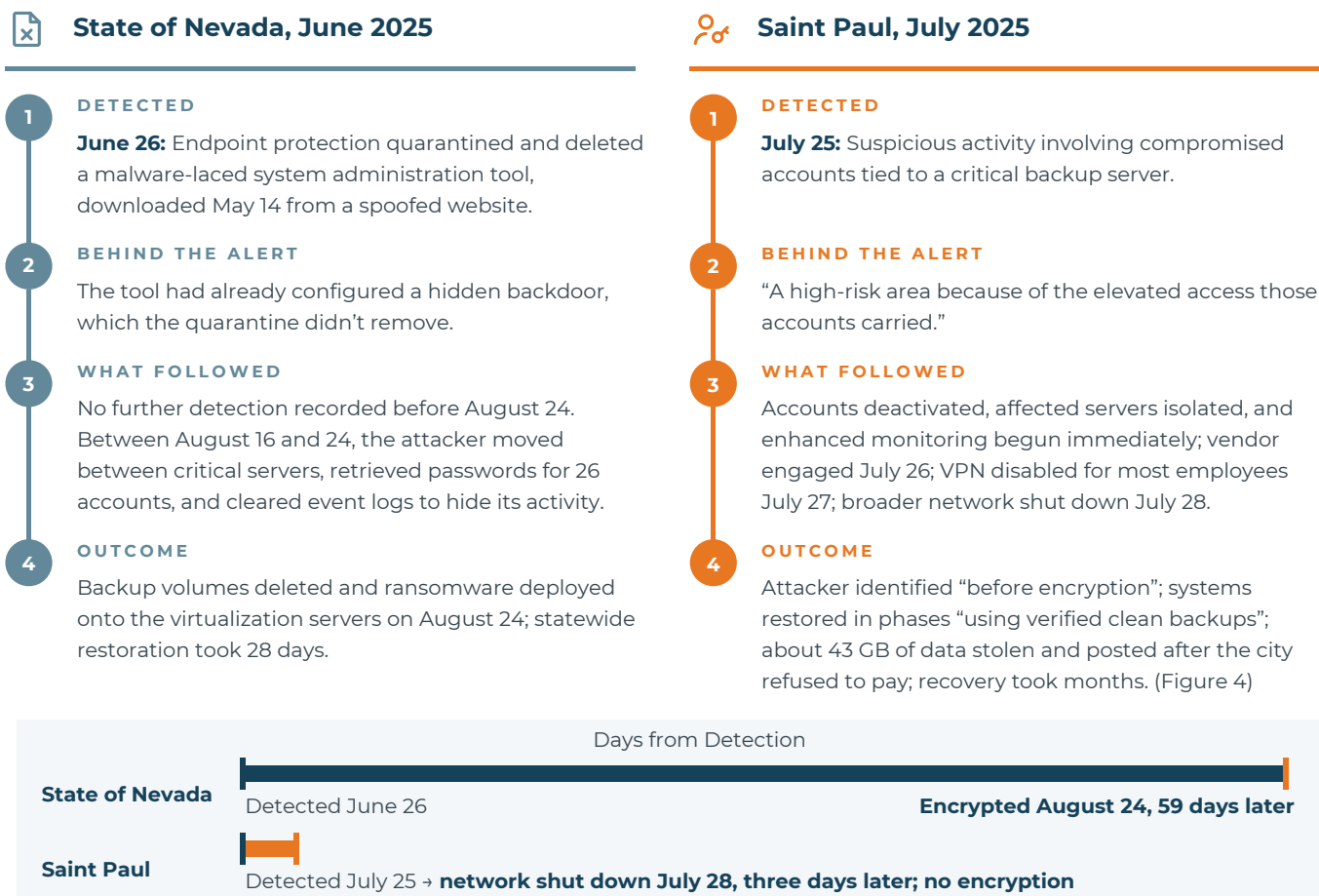
Detection and recognition are different capabilities, and plans take for granted that the first produces the second. Recognition is a judgment somebody makes, with partial information, about whether an alert is worth waking people up for.

Again, the Nevada incident shows the difference. The earliest evidence of the intruder dates to May 14, 2025, when a state employee downloaded a malware-laced version of a system administration tool from a website posing as the legitimate one. On June 26, the state's endpoint protection quarantined and deleted the tool. But the tool had already configured a hidden backdoor, which was not removed and stayed active. The after-action report records no further detection before the outage on August 24.³ An alert that closes as quarantined reads as a success, which makes it easy to stop looking before anyone asks what the tool had already set up.

The City of Saint Paul, Minnesota, read its first signal differently. On July 25, 2025, the city's cybersecurity systems detected suspicious activity involving compromised accounts tied to a critical backup server, which the city described as a high-risk area "because of the elevated access those accounts carried." It engaged a vendor the next day, disabled VPN access for most employees the day after that, and on July 28 shut down its broader network to stop the attacker.⁶ The city took the signal seriously because it knew what those accounts could reach. Recognizing it early didn't make the recovery short, as Figure 4 on page 11 shows. It did mean the city was the one deciding when its network came down, and shutting down a city's network three days in is a call someone has to be authorized to make.

FIGURE 3: TWO DETECTIONS

Both security tools caught something. Only one detection started the response.



This is also the assumption a tabletop exercise is least suited to test on its own. An exercise tests the response once the room knows there is an incident. Recognition happens earlier, before anyone has called the meeting, so it needs its own check: what the monitoring solution sees, who reviews it and how quickly, and what happens to an alert after a tool reports it handled. That check has two parts. The first looks back: pull a recent sample of alerts that were closed as quarantined or resolved, and for each one, find out what the threat did before it was caught and whether anyone checked. The second looks forward: run a harmless simulation of attacker activity, ideally outside business hours, and see whether it raises an alert and how long that alert takes to reach someone with the authority to act on it.

2.4 That recovery time is restoration time

Recovery objectives are usually built around how long it takes to bring the data back. Restoring the data is the beginning. What follows is rebuilds, revalidation, reconnection, reconciliation of everything that changed while systems were down, and a series of judgment calls about when a given system is safe to turn back on. None of that appears in the objective, and most of it can't be compressed by buying faster storage.

There is also a gap between what IT calls recovered and what everyone else does. A finance system that is back but missing three days of transactions, or a permitting system whose queue has to be rebuilt by hand, is restored in IT's sense and nobody else's. The difference is often measured in weeks of manual work by people who don't report to IT.

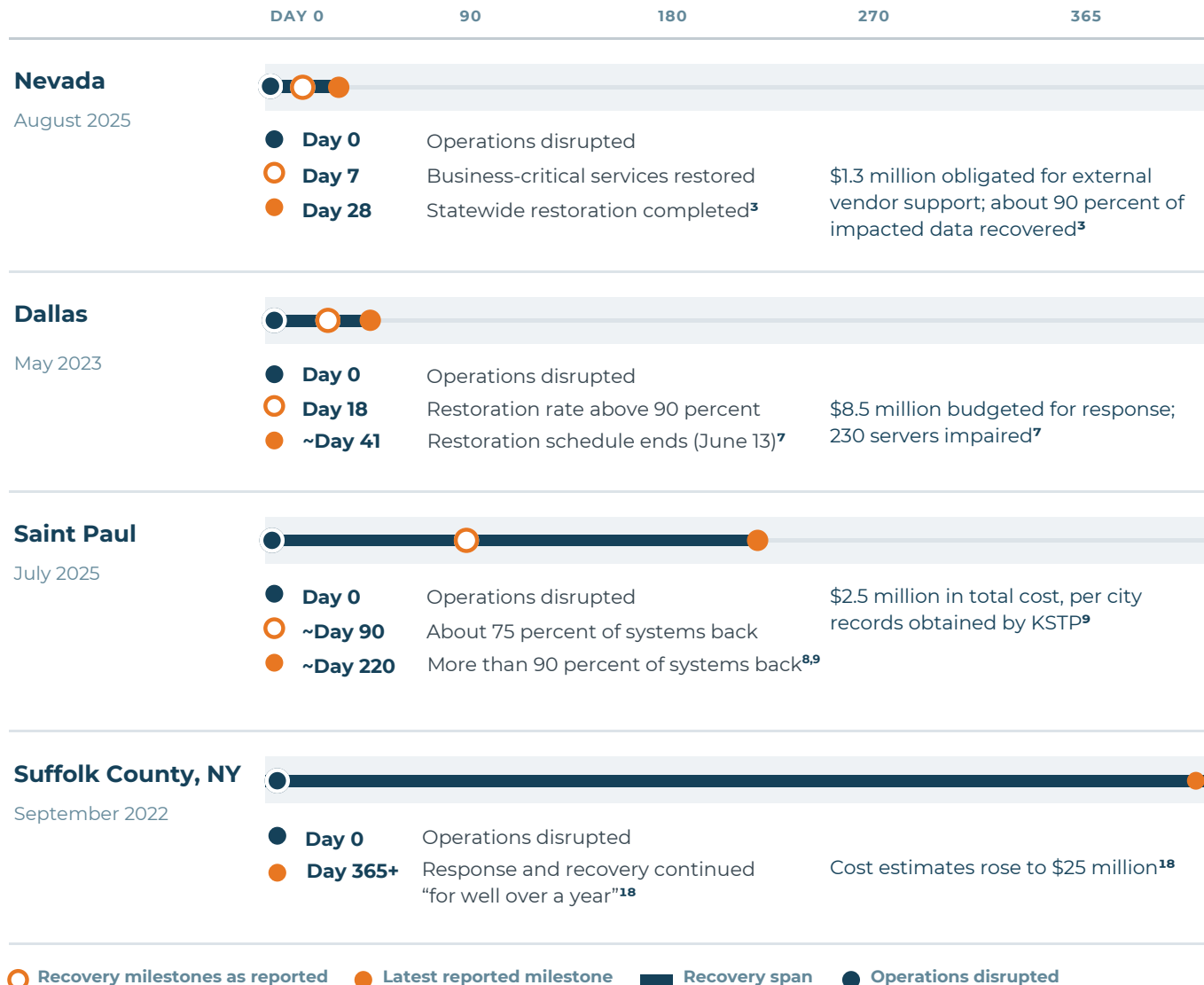
A recovery objective is one number. Three of the four organizations in Figure 4 reported recovery in stages. Nevada had business-critical services back within seven days and completed statewide restoration on day 28, and the recovery work included a full rebuild of Active Directory.³ The City of Dallas, Texas, reported a restoration rate above 90 percent within 18 days of its May 2023 attack, but the restoration schedule in its after-action review runs through mid-June, about six weeks after the attack was detected.⁷ Saint Paul reported about three-quarters of its systems back online in late October 2025, three months after the shutdown, and more than 90 percent in early March 2026.^{8,9}

Nevada recovered about 90 percent of the impacted data. The rest stayed under the state's control but was never recovered, and the state judged that essential services didn't need it.³ That is a recovery decision too, and a recovery objective has no field for it.

An organization that tells its board it can recover in 48 hours may only mean it can restore its data in 48 hours. If so, it has made a promise it won't be able to keep, and the board will learn that during the incident.

FIGURE 4

How long recovery took



Days counted from the day operations were disrupted; "~" marks an estimate from the reported date

Figures as reported by each organization or, for Saint Paul, by KSTP from city statements and public records. These incidents differ in scale, sector, and circumstance, and the numbers are not comparable to one another. Where an organization reported more than one milestone, the milestones were weeks or months apart.

3. Two ways to find your gaps before an incident does

Most of the gaps above can be found in advance, without an incident. Two good places to start are a [document-level review](#) and an [executive tabletop exercise](#), and Securance has published a separate case study on each.



Document-level review

A document-level review compares the plan to the environment it claims to describe: the real systems, people, and dependencies. In the first companion case study, a National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) gap analysis and incident response plan review for a national printing and direct-mail company found that the plan's escalation contact list predated a reorganization, with several "first call" roles belonging to people no longer in them. The plan also referenced backups without documenting how, or how often, their integrity was verified.



Executive tabletop exercise

An executive tabletop exercise puts the people named in the plan in a room with incomplete information and a running clock. In the second companion case study, a hypothetical ransomware scenario took a regional food and beverage manufacturer's executives, legal counsel, and communications team through the calls a true incident would force. They left with a clear answer on who has the authority to approve a ransom-negotiation ceiling, a decision that until then had lived in assumption.

One finds what the plan gets wrong. The other finds what the organization gets wrong. Either one costs a fraction of what the organizations in Figure 4 spent.

4. Case study: real-world ransomware response and recovery

The case study below comes from a ransomware response Securance led for a city government. Three of the decisions that determined how it went map onto the assumptions above: who would be in charge, which backups could be trusted, and what order the city came back in. All three were made in the middle of the response. The remaining assumption, recognition, isn't part of this story. By the time the city needed an outside team, the ransomware had already run.



The client

A mid-sized city government in the Southeast, serving both city and county residents through shared government network infrastructure — the kind of resource-constrained public sector IT environment where a written incident response plan often exists but has never been tested.



The challenge

The city experienced a live ransomware attack without the benefit of a prior tabletop exercise. Ransomware entered through a phishing email, then spread and encrypted systems across city and county government networks, disrupting core business operations. With operations down and the scope of the compromise still unclear, the city needed an experienced outside team to lead the response rather than improvising one under pressure.

The Securance solution



Ran the incident response war room, coordinating the city's internal IT staff and other responders through a single command structure.



Directed containment and forensic evidence preservation for law enforcement and insurance, in parallel with recovery planning.



Determined which systems could be restored from clean backups versus which required rebuilding from scratch, and directed the reimaging of the affected servers and workstations.



Restored services in order of business criticality, verifying each system clean before reconnecting it.



Following recovery, was engaged as the city's ongoing virtual chief information security officer (vCISO) to convert the incident into a lasting security program rather than a one-time fix.

Client success

Core business systems were restored within about a week. Securance still holds the vCISO role today, and in that capacity has helped the city build a formal incident response program and stand up a virtual security operations center (vSOC) — moving the city from crisis response to continuous monitoring and readiness. The city has not experienced a ransomware incident since.

5. What this engagement shows every organization that hasn't been tested yet



Command structure is something you build now, or at 3 a.m.

The first thing the engagement produced was organizational: a war room, with one command structure coordinating the city's IT staff and every other responder, so that decisions ran through one place.

An organization that has never rehearsed builds its command structure during an incident, and the cost of doing that can be hard to pin down. It shows up as a slower response, with the delay spread across dozens of small moments of working out who decides. Next to the more dramatic parts of the response, those moments are easy to overlook, so they're less likely to come up in the after-action review. The organization can then find itself running the same slow response twice.



Having backups doesn't settle which ones to trust

One of the engagement's core tasks was determining which systems could be restored from clean backups and which had to be rebuilt from scratch.

A backup policy says what gets backed up and how often. It doesn't say whether a particular backup can be trusted after an intrusion, which depends on whether the attacker was already inside when it was taken and whether restoring it would reinfect a network that has just been cleaned. Nevada's intruder was in the environment for more than three months before the ransomware ran,³ and a backup of an affected system taken at any point in that window would have carried the foothold with it.

Attackers now go after backups directly, as the Gunra and Nevada attacks showed, so the safe posture during a response is that every backup is suspect until someone establishes otherwise. Establishing this requires evidence of when the intrusion began, and that evidence arrives in pieces over the first several days. The restoration decisions made earliest are the ones made with the least information.

Sequencing is a governance decision

To avoid reintroducing risk onto a network that was still compromised, Securance sequenced the city's restoration by service criticality rather than by what was fastest to bring back online. It is the least intuitive decision in the response, and the one an unrehearsed team is most likely to get wrong, because under pressure, the instinct is to bring back whatever is ready first.

Which services come back first is a decision about who the organization serves, what it is legally obligated to do, and what it can defend at the next council or board meeting. In an organization that hasn't agreed on that order, the decision gets made by whoever happens to be in the room when it can no longer be put off. An order settled in advance, with the business owners who will have to live with it, takes the most contested conversation of the week out of the worst moment to have it.

Many organizations have some version of a priority list. Michigan's is the State of Michigan Application Prioritization for Recovery, created to rank critical applications and services for recovery after a large-scale outage, and the same audit that opened this paper found that its oversight needed improvement.¹ A list sets tiers. The order within and across them still gets argued out during the incident. In Nevada, that argument ran through the governor's office, which set priorities each day around life and safety, statutory and fiscal obligations, and public-facing continuity.³

The testing gets bought either way

The engagement didn't end when systems came back online. The city kept Securance on as its vCISO, and the work that followed included building a formal incident response program and a virtual security operations center.

That order of events is common. In IBM's 2026 Cost of a Data Breach study, 64 percent of breached organizations said they would increase security investment afterward, and among them, incident response plans and testing was the second most common area named for investment, identified by 43 percent.¹⁰ Many organizations buy the testing eventually. What varies is whether they buy it before the incident or after. After, it costs more and proves less, because the incident has already answered the question the exercise would have asked.

64%

of breached organizations said they would increase security investment after the breach

43%

of those planning to increase investment named incident response plans and testing, second only to hiring skilled security specialists

FIGURE 5

Four questions to answer before someone else asks them.

- 1 What is the last date on which someone restored a critical system from backup, end to end, and timed it?
- 2 Who, by name, can take a production system offline at 3 a.m. without waiting for a meeting, and have they ever done it in a rehearsal?
- 3 When a security tool reports a threat handled, who checks what it did before it was caught?
- 4 If you could bring back only five systems this week, which five, and who signs off on that list?

6. Why this matters to the people who answer for it

Everything above is an operational argument. It is also a governance argument now, and the pressure comes from four directions.



The decision now falls to the governing body. Ohio's cybersecurity law, effective September 30, 2025, bars a political subdivision from paying a ransom unless its legislative authority formally approves the payment in a resolution or ordinance that "specifically states why the payment or compliance with the ransom demand is in the best interest of the political subdivision."¹¹ Read that as an operational requirement and it says something stark: a council that has never discussed the question will be asked to vote on it, in public, under a countdown. Whether it can make an effective determination is a readiness question, and readiness is not something a council can acquire during the incident. A position on payment, an understanding of what the organization can restore without paying, and a procedure for convening quickly all have to exist beforehand.



The auditor is already writing it up. In February 2026, the New York State Comptroller reported that a city school district's board and officials had not developed and adopted an IT contingency plan, and recommended adopting one that is periodically tested and updated as needed.¹² As the Comptroller's audits routinely do, the report assigned the board responsibility for initiating corrective action, with a written corrective action plan due within 90 days. The finding names the board as accountable, in a public document.



The insurer asks on the form. Beazley's ransomware supplemental application asks whether the applicant has a business continuity or disaster recovery plan that includes responding to cybersecurity threats and was created or updated within the past two years. Follow-up questions ask if the applicant has exercised the plan with its incident response team, conducted a tabletop exercise in the past two years, and included ransomware in that exercise.¹³ The form asks about the plan and the exercise separately because they are different facts.



In several sectors, testing is required by law. Texas requires state agencies and public institutions of higher education to exercise or test incident response plans at least annually.¹⁴ The North American Electric Reliability Corporation (NERC) requires entities with high- and medium-impact Bulk Electric System (BES) Cyber Systems to test each cybersecurity incident response plan at least once every 15 calendar months, and responding to a reportable incident counts as a test.¹⁵ HIPAA's Security Rule has called for procedures for periodic testing and revision of contingency plans since 2003, as an addressable specification.¹⁶ HHS proposed in January 2025 to make that testing required, at least once every 12 months, but the rule had not been finalized when this paper went to press.¹⁶ The FTC Safeguards Rule, which covers non-bank financial institutions and, through their Title IV participation agreements, colleges and universities, doesn't require testing the incident response plan. For institutions holding information on 5,000 or more consumers, though, it does require the plan to define "clear roles, responsibilities, and levels of decision-making authority," and the institution to provide an annual written report to the board.¹⁷

FIGURE 6

Who is asking, and what they ask

WHO IS ASKING	WHAT THEY REQUIRE OR ASK	THE ANSWER AN UNTESTED ORGANIZATION HAS TO GIVE
 The governing body (Ohio political subdivisions)	Formal approval by the legislative authority, in a resolution or ordinance stating why paying is in the subdivision's best interest, before any ransom payment.	<i>"We have never discussed this, and we are discussing it now, in public, under a countdown."</i>
 The state auditor (New York school district, February 2026)	A developed and adopted IT contingency plan, distributed to responsible parties and periodically tested, with the board responsible for corrective action.	<i>"We have a plan on file. We can't show when anyone last tested it."</i>
 The insurer (Beazley ransomware supplemental application)	A continuity or recovery plan covering cyber threats, created or updated in the past two years; exercises run through it start to finish; a cybersecurity tabletop exercise in the past two years, and whether it covered ransomware.	<i>"Yes to the first question. No to the follow-up."</i>
 The sector regulator (Texas DIR, NERC, HHS)	Annual exercise or test (Texas); a test at least every 15 calendar months for high- and medium-impact systems (NERC); periodic testing and revision of contingency plans (HIPAA).	<i>"We can produce the plan. We can't produce the test results."</i>

None of this requires a board to become technical. The questions it needs answered can be asked in plain language: when the organization last restored a critical system and timed it, and who, by name, would take systems offline, check what a threat did before a tool caught it, and sign off on which systems come back first.

The board question was never "do we have a plan." The answer is almost always yes. The question is when it was last run, by whom, against what, and what changed afterward.

7. Next steps

01

You can start this without us. Answer the four questions in Figure 5 this month, honestly, with the people who would be named in the response sitting in the room. If any question produces a pause, that pause is your finding.

02

Then schedule the exercise. The Ransomware Tabletop Exercise Prep Checklist in Figure 7 covers what to prepare, who to invite, and how to run the session, and the two companion case studies show what a [document-level review](#) and an [executive tabletop exercise](#) each produce in practice.

03

While an exercise surfaces structural gaps, a Securance ransomware readiness assessment goes further. Not only do we review your disaster recovery and incident response plans and run a ransomware tabletop exercise, we also assess and inventory your backups, review ransomware quarantine capabilities and network and endpoint monitoring, evaluate endpoint configuration and your endpoint detection and response (EDR) solution, and assess security awareness training. We map controls and policies to the NIST CSF and technical findings to the MITRE ATT&CK framework, so you can see exactly where an attacker would gain a foothold, escalate, and spread.

Book a readiness assessment or a tabletop exercise at
securanceconsulting.com/ransomware-readiness.

FIGURE 7

The Ransomware Tabletop Checklist

Ransomware decisions come fast. Practice them first.



BEFORE THE EXERCISE

- ☐ Agree on what the exercise is meant to prove and how you'll judge success.
- ☐ Determine with counsel whether the exercise and its findings will be covered under attorney-client privilege — the after-action report is discoverable otherwise. This is a live question, not a formality, for CISOs in regulated sectors.
- ☐ Identify a cross-functional participant list: IT/security lead, network or systems administrator, legal counsel, communications/PR, and at least one executive sponsor.
- ☐ Pull your current incident response (IR) plan, network diagram, and backup/recovery architecture documentation.
- ☐ Confirm which backups are isolated (air-gapped or immutable) from the production network.
- ☐ Locate your cyber insurance policy's notification window and required carrier contacts.
- ☐ Define which systems and business units the scenario will cover.
- ☐ Set a date and block off three to four hours. Full attendance matters more than a longer session.
- ☐ Assign a note-taker who is not a scenario participant.



DURING THE EXERCISE

- ☐ Start with a realistic initial-alert scenario calibrated to your environment, not a generic template.
- ☐ Introduce escalations and complications in stages. Don't reveal the full scenario up front.
- ☐ At each stage, ask explicitly: "What does the plan say happens next, and who is responsible?"
- ☐ Track every point where the group is unsure, disagrees, or has to guess.
- ☐ Confirm decision authority for containment actions, including whether it changes on nights and weekends.
- ☐ Test the communication plan by drafting a sample customer or regulator notification.



AFTER THE EXERCISE

- ☐ Compile every uncertain or failed moment as a formal, written finding.
- ☐ Write findings up in plain language, organized by owner (IT, legal, communications, executive). A tabletop exercise surfaces decision-rights and coordination gaps, not technical findings, so this isn't a framework crosswalk.
- ☐ Assign a named owner and a target remediation date to every finding.
- ☐ Update the IR plan.
- ☐ Schedule the next tabletop exercise now — 12 months out, on the calendar, not "sometime next year."

securanceconsulting.com/ransomware-readiness

8. About Securance

Since 2002, we've helped organizations secure their data and systems and manage compliance risk. For ransomware, that means finding out whether a response plan holds up before an attacker tests it. Every engagement is led and carried out by consultants with 15 or more years of experience.

If an incident is already underway, we also provide incident response, with or without a retainer, and mobilize experts within eight hours of notification. Before it comes to that, a tabletop exercise shows whether the people named in your plan can make the decisions it assigns them, and a readiness assessment checks the plan against the environment it will have to run in, from backups to monitoring to endpoint detection.



BEFORE

Tabletop exercise

Shows whether the people named in your plan can make the decisions it assigns them



BEFORE

Readiness assessment

Checks the plan against the environment it will have to run in, from backups to monitoring to endpoint detection



DURING

Incident response

With or without a retainer, experts mobilized within eight hours of notification

Sources

1. Michigan Office of the Auditor General, Performance Audit Report: Disaster Recovery of IT Systems, Department of Technology, Management, and Budget, Report No. 171-0511-24, August 2025. <https://audgen.michigan.gov/wp-content/uploads/2025/08/r171051124-893563-1.pdf>
2. Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, Department of Defense Cyber Crime Center, National Security Agency, U.S. Secret Service, and Republic of Korea's National Police Agency, #StopRansomware: Gunra Ransomware, Joint Cybersecurity Advisory AA26-222A, August 10, 2026. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-222a>
3. State of Nevada, Governor's Technology Office, After Action Report: 2025 Statewide Cyber Incident, October 28, 2025 (released November 5, 2025). https://www.it.nv.gov/siteassets/itnew.nv.gov/content/governance/GTO_Statewide_Cyber_Event_AAR_Final.pdf
4. State of Nevada, Office of the Governor, "Nevada completes 28-day recovery from statewide cyber incident; refuses ransom and releases After-Action Report," press release, November 5, 2025. https://gov.nv.gov/Newsroom/PRs/2025/2025-11-05_nevada-completes-28-day-recovery-from-statewide-cyber-incident
5. State of Nevada, Governor's Technology Office, after-action executive briefing presented to the Nevada Commission on Homeland Security, February 6, 2026. https://www.oem.nv.gov/siteassets/oem.nv.gov/public-meetings/public-meetings-2026/homeland-security-2026/5_aar-executive-briefing.pdf
6. City of Saint Paul, Minnesota, Department of Emergency Management, "Cyber Incident Info Hub," last edited July 2, 2026. <https://www.stpaul.gov/departments/emergency-management/cyber-incident-info-hub>
7. City of Dallas, Department of Information and Technology Services, The City of Dallas Ransomware Incident: May 2023 – Incident Remediation Efforts and Resolution, after-action review, September 20, 2023. <https://dallascityhall.com/departments/ciservices/DCH%20Documents/dallas-after-action-review-slideshow-of-ransomware-attack.pdf>
8. KSTP, "City of St. Paul says '75%' of systems back after summer cyberattack; full cost not shared yet," October 22, 2025. <https://kstp.com/kstp-news/top-news/city-of-st-paul-says-75-of-systems-back-after-summer-cyberattack-full-cost-not-shared-yet/>
9. KSTP, "Cyberattack cost City of St. Paul \$2.5 million," March 6, 2026. <https://kstp.com/kstp-news/top-news/cyberattack-cost-city-of-st-paul-2-5-million/>
10. IBM, Cost of a Data Breach Report 2026, July 2026. <https://www.ibm.com/reports/data-breach>

11. Ohio Revised Code § 9.64, Cybersecurity programs of political subdivisions, effective September 30, 2025. <https://codes.ohio.gov/ohio-revised-code/section-9.64>
12. Office of the New York State Comptroller, Syracuse City School District: Information Technology, Report 2025M-129, February 2026. <https://www.osc.ny.gov/local-government/audits/school-district/2026/02/20/syracuse-city-school-district-information-technology-2025m-129>
13. Beazley Insurance Company, Inc., Ransomware Supplemental Application, Form F00765 (05/2022 edition), questions 45 and 46. https://www.beazley.com/globalassets/product-documents/application/ransomware_supplemental_application_v7.1_f00765_052022_ed.pdf
14. Texas Department of Information Resources, Security Control Standards Catalog, version 2.2, control IR-03, Incident Response Testing, required under 1 Texas Administrative Code §§ 202.26 (state agencies) and 202.76 (institutions of higher education). https://dir.texas.gov/sites/default/files/2025-09/Security%20Control%20Standards%20Catalog_v2.2.pdf
15. North American Electric Reliability Corporation, CIP-008-6: Cyber Security, Incident Reporting and Response Planning, Requirement R2, Part 2.1. <https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-008-6.pdf>
16. U.S. Department of Health and Human Services, HIPAA Security Rule, 45 C.F.R. § 164.308(a)(7)(ii)(D), Testing and revision procedures. <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.308> Proposed update: U.S. Department of Health and Human Services, Office for Civil Rights, “HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information,” notice of proposed rulemaking, 90 Fed. Reg. 898, January 6, 2025. <https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information>
17. Federal Trade Commission, Standards for Safeguarding Customer Information, 16 C.F.R. §§ 314.4(h), 314.4(i), and 314.6; U.S. Department of Education, Federal Student Aid, Electronic Announcement GENERAL-23-09, February 9, 2023. <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314/section-314.4> <https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2023-02-09/updates-gramm-leach-bliley-act-cybersecurity-requirements>
18. Suffolk County Legislature, Special Cyber Intrusion Investigation Committee, Report on the 2021–2022 Cyber-Attack on Suffolk County, September 12, 2024. <https://www.scnylegislature.us/DocumentCenter/View/118502/09122024-Report-On-The-2021-2022-Cyber-Attack-On-Suffolk-County-PDF>



Tested, Not Just Written
© 2026 Securace LLC. All Rights Reserved.



13916 Monroes Business Park, Suite 102, Tampa, FL 33635 • 877.578.0215
www.securaceconsulting.com

