

Cyber Incident Response Planning for Public Entities

A Cyber Incident Is Not the Time to Write Your Response Plan

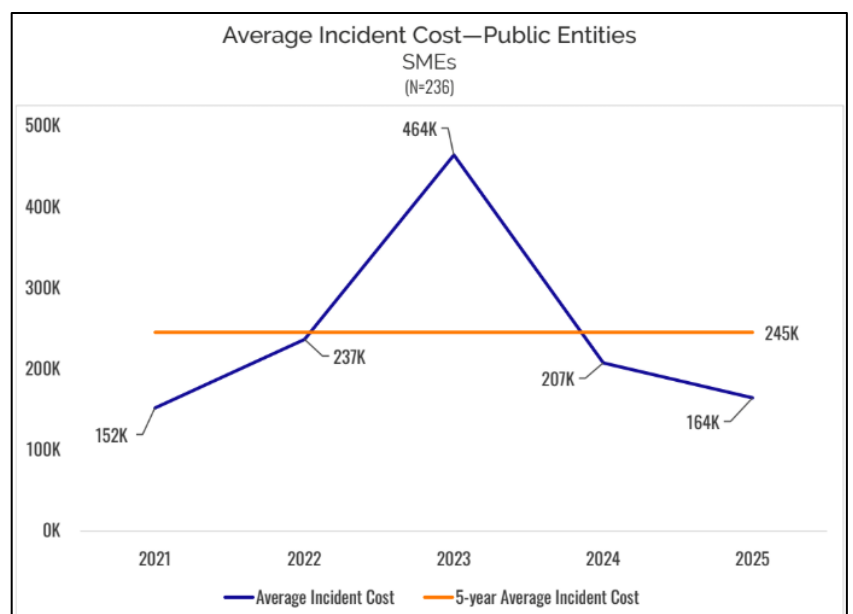
In February 2026, criminals impersonating a [trusted vendor tricked Dickinson Public Schools in North Dakota](#) into redirecting approximately **\$4.92 million** in building-fund payments to a fraudulent account. The business email compromise (BEC) scheme diverted two scheduled vendor payments before the district discovered the fraud and contacted law enforcement.

It is far from an isolated threat: the [FBI's Internet Crime Complaint Center](#) recorded **\$3.05 billion in reported BEC losses across 24,768 complaints in 2025**, making BEC the second-highest cybercrime category by reported losses. **Wire transfers and ACH accounted for 86% of the transaction types reported in BEC complaints.**

For public entities, that speed is the real danger. A single unverified email—one changed bank account, one urgent request to update payment details—can drain public funds before anyone realizes something is wrong.

NetDiligence's [2026 Cyber Claims Study](#), which analyzed 236 cyber insurance claims involving public entities, found that ransomware, [business email compromise](#) and wire transfer fraud were the leading causes of loss, with incident costs ranging from \$152k to \$6M with an average five-year cost of \$245k.

That is exactly where BEC policies, preparation and, an [incident response plan](#) (IRP) come in. A good cyber IRP, coupled with a BEC policy, is what stands between an attempted scam and an actual loss.



Why public entities need an actionable plan

During a cyber event, response teams may need to make consequential decisions under significant pressure. Leaders may be coordinating simultaneously with IT personnel, legal counsel, cyber insurers, law enforcement, forensic specialists, and PR communications teams.

Without a clear plan, valuable time may be lost answering basic questions:

- How can you activate your IRP for a crisis happening at 2am?
- Do you have the 24/7 hotline contacts and access to cyber crisis experts you will depend upon for response and recovery, such as your cloud provider, legal breach counsel, cyber forensic response, IT personnel and other experts and stakeholders?

- Are your experts pre-approved by cyber insurance coverage and do you understand required cyber claims reporting instructions?
- Which services must be restored first to protect residents and maintain operations?

A well-designed IRP does not eliminate every difficult decision. But it does help ensure that the right people can make those decisions with the right information—and without avoidable delays.

Five common incident response planning mistakes

1. Treating the plan as an IT-only document

Cyber incidents are operational and organizational events, not simply technical problems. An effective response may require participation from executive leadership, legal, finance, human resources, communications, risk management, public safety, records management and outside specialists.

The plan should clearly define each participant's role, responsibilities and decision-making authority before an incident occurs.

2. Starting with a generic template—and leaving it generic

A template can provide a helpful foundation, but it must reflect the organization's actual structure. Department names, escalation paths, insurance requirements, outside vendors, communication procedures and approval authorities should be customized.

The plan should also reflect the entity's essential services. A water utility, police department, public works operation and municipal finance office may have very different continuity and recovery priorities.

A plan that does not match how the entity really operates can create more confusion when it is needed most.

3. Storing the only copy on the network

If ransomware locks files, disables email or interrupts network access, a plan stored exclusively on those systems may be unavailable.

Authorized response team members should have a secure alternative way to access the plan, contact information, claims instructions, response procedures and key documents when normal systems are compromised.

The team should also establish an out-of-band communication method that does not depend on the organization's primary email or network environment.

4. Failing to maintain contact and insurance information

Staff members change roles. Vendors change. Phone numbers, after-hours contacts, cyber insurance policies and claims-reporting requirements are updated.

An outdated plan may send responders to the wrong person or cause them to miss important notification steps. Assign a plan owner and establish a recurring schedule for reviewing the plan, preferably at least annually and whenever there is a significant staffing, vendor or insurance change.

5. Never practicing the plan

A plan that has never been discussed or tested may not perform as expected during a real incident.

Tabletop exercises help participants understand their responsibilities, identify unclear procedures, test communication channels and uncover gaps while there is still time to correct them.

Exercises should address realistic scenarios, including ransomware, business email compromise, fraudulent payment instructions and attacks that disrupt essential public services. After each exercise—or actual incident—the organization should document lessons learned and update the plan.

Start with Resources Available to You Through NLC-RISC

NLC-RISC members are eligible for **complimentary access** to eRiskHub®, a cyber risk management portal, powered by [NetDiligence®](#), including cybersecurity planning and modeling tools, educational resources, exclusive offers, and much more through your NLC-RISC membership.

Explore and bookmark the NLC-RISC eRiskHub portal today at eRiskHub.com/NLC.

Get Started

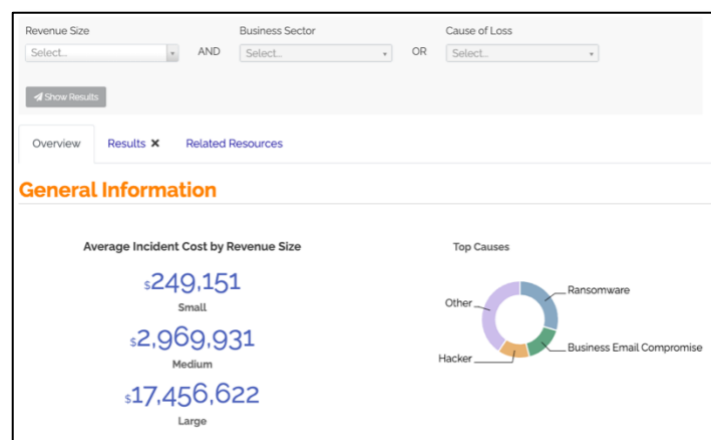
To register for your free access, simply register at the page above using [Access Code 13522](#).

- Please contact [Erin Clark](#) with any questions or for assistance registering for complimentary access.

Registered eRiskHub users can login to review incident response guidance, sample policies, planning tools and other materials designed to support cyber readiness.

Explore additional eRiskHub resources to address business email compromise (BEC) and wire fraud risk:

- **Example Business Email Compromise Policy:** A sample policy can be found in the eRiskHub that organizations can adapt to establish approval, verification and reporting expectations.
- **Business Email Compromise Fraud - What It Is and What You Can Do:** A Learning Center resource explaining how BEC schemes work and practical steps organizations can take to reduce risk.
- **Security Awareness Training:** With eRiskHub's new partnership with ESET, members can access engaging, self-paced training modules that help employees recognize phishing, BEC attempts and other social engineering tactics before they lead to a costly incident.
- **Claims Scenario Tool (shown right):** Model real-world loss scenarios, including incidents affecting public entities, that teams can use for awareness, training, and planning discussions.



Last but not least...Turn your cyber IR plan into an operational resource

For those ready to move beyond static response documents, [Breach Plan Connect®](#), also powered by NetDiligence®, provides a secure, cloud-hosted incident response planning platform with 24/7 mobile access. Organizations can **quickly customize an expert-vetted cyber incident response plan** to include their response teams, procedures, insurance information, key contacts, and supporting documents. All in one place.

Guided plan-building, response checklists, and playbooks for common incidents such as ransomware and business email compromise help teams stay prepared and act quickly. Authorized users can access critical plans, contacts, and procedures through the mobile app even when systems are compromised or unavailable.

Exclusive Offer for NLC-RISC Risk Pools & Member Municipalities

NLC-RISC risk pools and member municipalities can purchase an annual Breach Plan Connect subscription for:

\$900/year – including a 30-day free trial

Take advantage of 75% OFF the standard retail price of \$3,600/year

To learn more about the offer, log in to the NLC eRiskHub or contact Erin Clark at eclark@nlcmutual.com.

[Start Free Trial](#)

From static documents to a live, coordinated response system.

Breach Plan Connect keeps your team connected — anytime, anywhere.

What Fails in Real Incidents



Network down = plan inaccessible



IR plan buried in a binder or static PDF



No clear roles or contacts



Confusion on who to call during an incident



Plans rarely reviewed or tested



Hard to prove compliance or readiness



How Breach Plan Connect Fixes It



Out-of-band mobile app ensures full access even if your systems are locked by ransomware



Cloud-hosted plan available 24/7/365 from any device



Role-based plan builder auto-invites your internal team



Add Breach Coach®, DFIR, and PR contacts so they're aligned pre-incident



Automated reminders keep plan current and ready for audits



Downloadable IRP Certificate for insurers and regulators