XANTRION

CYBERSECURITY • IT SUPPORT

The Hidden Cyber Risks in Everyday Law Firm Operations

Five everyday processes you can improve

People. Exceptions. New tools. Security promises. Recovery.

Graham Roggli · Xantrion · ALA · October 8, 2026

Where I fit

XANTRION
CYBERSECURITY • IT SUPPORT

CONTEXT

Graham Roggli

Client Strategy Manager, Xantrion
groggli@xantrion.com • 510.588.8251

I help organizations connect technology decisions to business goals.

Understand what the business needs.

Identify opportunities and risks leadership should consider.

Turn technical issues into decisions people can act on.

Five moments where you can make a difference

XANTRION
CYBERSECURITY • IT SUPPORT

FIVE MOMENTS

	When this happens…	The process needs to answer…
01	**People change**	What access should change?
02	**The rules bend**	Who approves the exception, and what happens afterward?
03	**New tools appear**	How do we approve the intended use?
04	**Someone asks for proof**	What supports our answer?
05	**A critical system fails**	How will the firm keep working?

Recognize the situation, improve the process, check the result.

Three questions for any process

XANTRION
CYBERSECURITY • IT SUPPORT

THE FRAMEWORK

1

What should happen?

Clear expectations, including how exceptions are handled.

2

Who is responsible?

Someone owns the decision and the follow-through.

3

How do we know it happened?

A completed example, a review, or a realistic test.

Maturity means moving from defined, to consistent, to verified.

Defined

An owner and a checklist exist.

Consistent

It happens the same way every time.

Verified

A completed example or test proves it.

People change. Access should change too.

MOMENT 1 · PEOPLE CHANGE

01

A FAMILIAR SITUATION

An employee moves from finance into legal support.

Their new access is added. Their old access remains.

Years later, nobody can explain everything they can see.

On the record

Cash App (2021): a former employee still reached internal reports after leaving and downloaded them. Block notified 8.2 million customers.[1]

Where does access accumulate at your firm?

1. Block, Inc., SEC Form 8-K, April 4, 2022.

Make business changes trigger access changes

XANTRION
CYBERSECURITY • IT SUPPORT

MOMENT 1 · PEOPLE CHANGE

1

What should happen?

Joining, changing roles, leaving, or cancelling a start date triggers an access check.

2

Who is responsible?

A designated person initiates the request. The relevant business owner confirms what is needed. IT and system owners complete the changes.

3

How do we know it happened?

The request closes with confirmation, including access removed from the previous role.

Think through one recent departure or role change.

“Just this once” needs an ending

MOMENT 2 · THE RULES BEND

02

A FAMILIAR SITUATION

A colleague is unexpectedly out.

Someone needs temporary access to help with an urgent filing.

The access is granted. Nobody assigns its removal.

On the record

Wire instructions by email: a hacker inside a lawyer’s mailbox hid replies and redirected a settlement payment. A phone check protected the next one.[1]

What temporary exception has become permanent at your firm?

1. ABA Tort Trial & Insurance Practice Section, “Lawyer Liability for Wire Transfer Fraud,” The Brief, Spring 2025.

Give every exception an owner and a next step

XANTRION
CYBERSECURITY • IT SUPPORT

MOMENT 2 · THE RULES BEND

1

Record the decision

What is different from the normal standard, and why?

2

Name the approver

Who understands the risk and has authority to accept it?

3

Assign the follow-up

When does it end or get reviewed, and who completes that work?

Pro tip: Schedule removal when exception is granted.

Useful tools can arrive before the decision

MOMENT 3 · NEW TOOLS APPEAR

03

A FAMILIAR SITUATION

Someone finds an AI tool that saves time.

They start using it with client documents.

The firm has not agreed on the account, permitted information, or required review.

On the record

Mata v. Avianca (2023): a New York firm filed six cases ChatGPT had invented. The court fined the two lawyers and the firm $5,000.[1]

1. Mata v. Avianca, Inc., No. 22-cv-1461 (S.D.N.Y. June 22, 2023).

Build a route to an informed yes

MOMENT 3 · NEW TOOLS APPEAR

1

Ask about the proposed use

What will the tool do? What information will it receive or access?

2

Give the decision an owner

Who reviews the request, manages the account, and checks relevant client restrictions?

3

Define the conditions and exit

What uses are permitted? What requires human review? How do we remove access and address retained information?

Tell staff exactly what is approved, and how to request something new.

A checkbox can become a business promise

MOMENT 4 · SOMEONE ASKS FOR PROOF

04

A FAMILIAR SITUATION

A client or insurer asks:

"Is multifactor authentication required for all remote access?"

The firm knows it protects email.

Nobody has checked the other systems or exceptions.

On the record

Travelers v. ICS (2022): the CEO signed an MFA attestation. After ransomware, forensics found MFA only on the firewall, and the policy was voided.[1]

What would we need to verify before answering?

1. Travelers Prop. Cas. Co. of America v. Int'l Control Services, No. 22-cv-2145 (C.D. Ill. 2022).

Verify the claim before someone signs

MOMENT 4 · SOMEONE ASKS FOR PROOF

1

What should happen?

The answer matches the exact question, current arrangements, and known exceptions.

2

Who is responsible?

The control owner verifies the facts. The appropriate firm leader approves significant commitments.

3

How do we know?

Keep the supporting evidence, qualifications, and final submitted answer together.

Choose one significant claim from your last questionnaire and trace its support.

Documents and email are down tomorrow morning

XANTRION
CYBERSECURITY • IT SUPPORT

MOMENT 5 · A CRITICAL SYSTEM FAILS

05

THE SCENARIO

There is a filing due today.

- Who identifies the work that cannot wait?
- How do you reach staff?
- Who coordinates updates with IT?
- Which functions get restored first?

On the record

CrowdStrike (July 2024): a faulty security update crashed about 8.5 million Windows PCs. It was not an attack, yet many machines needed hands-on repair.[1]

What would the first hour look like at your firm?

1. Microsoft, estimate published July 20, 2024.

Test the ability to work again

MOMENT 5 · A CRITICAL SYSTEM FAILS

1

Agree on the business priorities

Which functions need to resume first? How long can they be unavailable? How much recent work can the firm tolerate losing?

2

Check the owners

Working devices, sign-in, documents, communications, vendors, and the people needed to recover.

3

Run a realistic exercise

Walk through the scenario with IT and the people doing the work. Test technical recovery where needed.

Assign the fixes and check completion.

Think through the effects of one important disruption.

Apply the framework to your firm

XANTRION
CYBERSECURITY • IT SUPPORT

TAKE-HOME WORK

Five processes. Can you answer all three questions?

Process	What should happen?	Who is responsible?	How do we know?
People and access			
Exceptions			
New tools and AI			
Client and insurer answers			
Recovery			

Take note of anything you are assuming or cannot yet answer.

Turn one uncertainty into one action

TAKE-HOME WORK

Choose something important enough to check. Write down:

1. The question you need answered.
2. The person who can help answer it.
3. The example or evidence you want to see.
4. When you will have the conversation.

Example

"Next week, ask our offboarding owner to walk through a recent departure, including separate vendor accounts and confirmation of removal."

Put that conversation on your calendar.

XANTRION
CYBERSECURITY • IT SUPPORT

Q&A

Questions and discussion

1. What should happen?
2. Who is responsible?
3. How do we know it happened?

You can use these questions in your next operational conversation.

Graham Roggli
groggli@xantrion.com • 510.588.8251