IMAGEQUEST℠

EMERGENCY DRILLS

TABLETOP EXERCISES

Have you actually practiced your Security Incident Response Plan?

Imagine this: You're in your office, in the middle of a major client project, when Bob in IT calls you.

Your vendor, "Acme Accounting Software, Inc.," has suffered an "incident." Details are few, and a security team is investigating.

However, some firm and client data probably have been compromised, including some of your client's financial records.

By Milton Bartley,
ImageQuest Co-Founder, President & CEO

What is the first thing you should do in response?

Have you and your team planned for such an event?

The shock of a situation such as this could paralyze you – and plunge your team into confusion.

You can waste a lot of valuable time and energy dealing with this problem if you and your team haven't thought in advance about what you would do – and should do.

This scenario appeared to play out this spring when accounting software giant Wolters Kluwer's CCH SureTax and other programs suffered a malware attack. Thousands of CPAs, accountants and tax preparers working

to meet a federal tax filing deadline found themselves unable to work mere days before returns were due.

Worse, Wolters Kluwer drew criticism for going silent about the attack. Accounting Today called it "a case study in how not to communicate with customers over a hack." Customers described the stress they felt seeing potential penalties ahead for unhappy clients. (The IRS ultimately offered a filing extension due to the incident.)

Even Wolters Kluwer employees struggled to find out what was going on at first and couldn't answer the flood of customer questions. The initial days of the malware attack were highly stressful for clients and employees alike.

While Wolters Kluwer, a global corporation, eventually resolved the outage, recovery might not be so easy for smaller, regional organizations. Going silent or inoperable during an incident could prove disastrous – from loss of income, loss of customers, and potentially loss of trust in the marketplace.

Thus, it is imperative to know in advance what you need to do to respond – and recover.

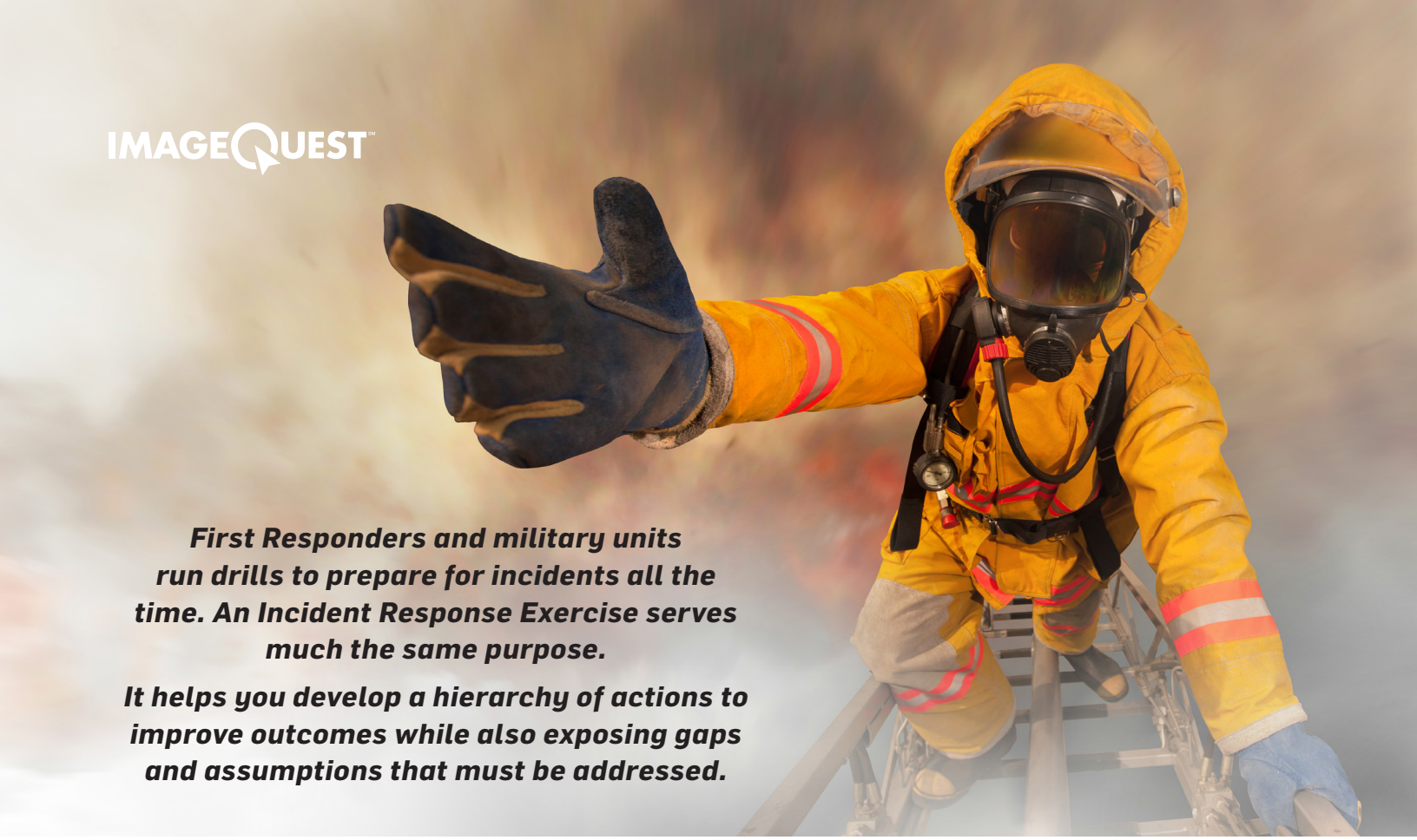
A recent IBM Security-Ponemon Institute study found that having a plan for responding to a data incident can save organizations a third of the costs of the incident – which can average in the millions of dollars.

And it makes sense – after all, First Responders and military units run drills to prepare for incidents all the time. An Incident Response Exercise serves much the same purpose. It helps you develop a hierarchy of actions to improve outcomes while also exposing gaps and assumptions that must be addressed.

Yet sometimes organizations task someone to write an Incident Response/Disaster Recovery plan - and then file it away and never practice it.

If your organization is a bank – you risk your board of directors failing their fiduciary responsibility to ensure your bank's stability

A recent IBM Security-Ponemon Institute study found that having a plan for responding to a data incident can save organizations a third of the costs of the incident – which can average in the millions of dollars.



and continued operations. Similarly, if you run a law firm or a healthcare provider, you have a critical responsibility to your clients for your organization to be there for them during and after an incident.

An untested plan is not an action plan. It is a collection of suggestions.

We do Incident Response or "Tabletop" Exercises with our clients. It's always instructive to discover decision points that either requires something to be established in advance (the right law enforcement contact, for example) or decision points that cannot be executed because of an unexpected problem (no communications available, for example.)

Our exercises expose steps that must be re-ordered, additional executives who need to be involved, or other contacts that must be on file. We follow the U.S. government's National Institute of Standards and Technology's recommendations for Tabletop Exercises.

Our exercises, per the NIST recommendations, take several hours and require the involvement of key people – including executives and board members.

"We find it can be easier to schedule and attain buy-in from leadership," said Milton Bartley, ImageQuest Co-Founder, President & CEO. "They prefer the exercise be run by an experienced third-party that can facilitate an accurate scenario. It's important your operating leadership team, your board, and your key department heads are involved and aligned in developing and practicing your response plan."

Having a plan also helps you handle crucial customer notification. Your clients will have expectations of timely notification and established remediation plans.

How do you communicate with them? A statement hidden somewhere on your website? Or an immediate notification that reassures them you've taken the right steps to limit their losses? What is the best way to provide great customer service when you have bad news?

We also like to add real-life scenarios to our client exercises. For example, what if your

incident is ransomware that shuts down all your communications systems – including your phones? What if you need to take specific steps to preserve evidence in the first minutes – and failing to do so costs you valuable evidence and recovery time? What if a leak leads to media queries?

What if, in the above example, the incident actually began two months ago - but you don't learn that's the case until 24 hours later? In that example, you may have communicated to clients one thing – and now you must revise the statement.

Your organization needs to continue to function and present a stable front to the community. If everyone on the executive team is fighting the incident response fire, will outsiders see that stable front? Or will people start whispering that something is going on at your business?

Simulation exercises, especially those run by a third-party, can bring these problems to light. In the low-stress environment of rehearsal, you can review and assess where you need to make changes and improvements, and your team members will better understand their roles.

Our clients who conduct these exercises tell us they appreciate learning "how to create action without causing panic." In several cases, organizations have taken the exercise to another level altogether, by having their internal management team conduct mini-incident response exercises in small groups.

Those leaders then reassemble and share notes and best practices from the individual meetings. This type of internal activity helps solidify the importance of security awareness and incident response throughout the organization.

Don't lose precious time and money by being unprepared for an incident. A well-rehearsed exercise will save you and your firm a lot of grief and costs down the road.