Racing Against Ransomware: Why Every Department Must Be Ready

Cybersecurity incidents are no longer limited to the IT department. A cyber-attack doesn't just disrupt systems, it sends shockwaves across the organization, touching finance, HR, legal, communications, operations, executive leadership and of course, customers and everyday people. In those moments, the difference between a manageable incident and a full-blown crisis is not just technology, but how people at every level respond.

True resilience comes from organizational readiness, but how do you get there? Cybersecurity is everyone's responsibility, far beyond just the data center.

Cyber Incidents: It's Not If an attack will happen, It's When..

When an attack hits, the first instinct is often "What can IT do?" But the reality is much broader:

- Executives must weigh ransom demands, operational downtime, and long-term reputational risks.
- Finance must assess recovery costs versus paying attackers.
- HR must keep employees informed and productive.
- Communications must address customers, stakeholders, and the press.
- Every employee must know how to recognize and report suspicious activity,

A ransomware attack becomes an organizational stress test. Leaving preparation solely to IT creates gaps that attackers are quick to exploit.

Walking in the C-Suite's Shoes

One of the most powerful lessons in training is experiencing the decisions leaders face under pressure. No one knows how executives or board members will react in a live incident:

- Do they authorize ransom payments?
- Do they prioritize operational continuity, legal obligations, or reputation management?
- Do they act quickly—or hesitate, hoping to buy time?

These choices shape the outcome and ripple across the company.

Our **Race Against Ransomware** tabletop exercise engages IT, executives, department leaders, and end users alike. Participants "step into C-suite's shoes", gaining insights into executive decision-making. By simulating the weight of those choices, employees better understand the complexity of cyber crises, and leaders gain a safe environment to practice making them. This hands-on training provides perspectives that cannot be taught in a classroom. It' a rare opportunity to see not just what a company goes through, but why decisions are made, and how they impact the entire organization.

Benefits of a Full-Organization Exercise

- Validates the Playbook Across Functions – Ensures IT, legal, finance, HR, and communications can act in sync.
- Builds Empathy and Awareness – Employees feel the pressures leaders face.
- Strengthens Communication Under Pressure – Aligns messaging internally and externally.
- Empowers End Users – Every employee plays a key role in detection and reporting.
- Fosters a Culture of Readiness – Security becomes a shared responsibility, not an isolated IT concern.

PKA Technologies: Preparing Every Department

For more than three decades, PKA Technologies has helped organizations modernize infrastructure and prepare their people. Our tabletop exercises ensure every department understands its role, every employee feels empowered, and every leader gains practical experience in making tough choices.

Because in the Race Against Ransomware, it's not just IT on the clock, it's everyone. It's not if an attack will happen, but how ready your organization will be when it does.

Want to learn more? Contact Eli Katz at Eli.Katz@pkatech.com or (845) 738-2317.