See Jane SECURE

Sometimes it's about keeping employees safe in spite of themselves. Here's how Jane does it.
Meet Joe. Joe doesn't always follow the best cybersecurity practices.

Meet Jane. Jane is always cleaning up after Joe's cybersecurity messes.
Here’s Joe’s approach to passwords.

Joe uses PASSWORD on everything.

Joe uses the same password everywhere.

Joe shares his password.

See how Jane responds.

1. **Security Awareness Training**
   Jane gives her employees the knowledge and skills they need to protect themselves AND the organization—because it’s built to fit many types of learning styles. Plus, this training helps her meet compliance requirements, minimize risks and maximize data security.
   
   Get Training

2. **Participating in Cybersecurity Awareness Month (CAM)**
   Jane sends Joe and other employees CAM resources like this video and encourages them to participate in weekly cybersecurity challenges like #BeCyberSmart. They’ll better understand how vulnerable they are and how cybersecurity is everyone’s responsibility.
   
   More CAM Resources

3. **Penetration Testing**
   Jane knows her organization would benefit from comprehensive and targeted penetration testing. She reaches out to her trusted cybersecurity partner, Optiv, to help set up overall vulnerability assessments and advanced breach simulations.
   
   Read the Brief
However some of Joe’s bad cybersecurity practices may have spread...

Joe’s now a VP with a growing team, and he is training them himself.

OR

Uh oh. Joe left the company and can still get into the network.

Now see how Jane prevents this.

1. Attack Surface Management
   Jane uses Optiv’s Attack Surface Management services with differential penetration testing — giving a full comprehensive baseline — and then continually identifying and testing her new or changing attack surface. She gets visibility into new vulnerabilities introduced by new systems and services or configuration changes implemented between cycles. Optiv also offers SME hours to help strengthen her program.

2. Security Awareness Training
   Jane’s earlier training never stops, enabling her employees with knowledge and skills to protect themselves and the organization.

Learn More

Get Training
Joe still goes “wild, wild West” sometimes.

Joe found a flash drive and puts it into his laptop.

Joe loses his company-issued flash drive and doesn’t report it.

Joe accesses things he’s not supposed to.

Joe keeps IT hopping. He sets off alerts right and left and doesn’t get why he’s a distraction from real breaches.
See Jane defend.

1. **Advanced Fusion Center**
   Jane works with Optiv, identifying real threats in her environment, providing context and eliminating them. With prejudice. Also, with deep data analytics and full-packet capture technology that drives 24x7 threat monitoring, alert investigation and event and file analysis. We co-manage Jane’s packet-capture platform to address change requests, data source classification and groupings, native reporting, platform incident management, problem management, health checks and release management.

   [Watch the Video]

2. **Digital Access Management**
   Provides secure and uniform access to business systems and resources with custom risk-based access policy enforcement. With it, Joe won’t be able to access files he has no business accessing.

   [Read the Brief]

3. **Threat Monitoring Service**
   Jane’s team has alert fatigue and it’s not getting better. She needs a more proactive, tactical defense. Optiv’s Threat Monitoring Service would help her identify vulnerabilities, and that can assist with developing a strategic roadmap.

   [Learn More]

4. **Incident Response**
   With insider threats increasing, Jane needs a partner who evolves as attackers adapt their tactics. Optiv’s Incident Response team works with cloud-based technologies to expedite rapid response and hunt for intruders. Optiv’s Threat Management community diagnoses and responds to attacker tactics techniques and procedures (TTPs) faster than traditional incident response teams.

   [Download the Brief]
And then Joe starts working remotely...

...in his basement. On his own network. Hackers rejoice! In a few months he could work in a coffee shop on “FREEWiFi.”

Joe insists on using his own phone for work.

Work From Home Strategy
Jane rushed to enable remote access for Joe and the rest of the organization during COVID. To keep her network safe, Optiv offers three remote work strategies: expand existing access, create alternate access methods and infrastructure redesign. Jane may already be doing some of this, but she may need a refresher.

Work from Home Assessment
Jane can identify, review and prioritize strategic risks associated with newly remote users, making sure they're safe.

Digital Access Management
If Joe has Multifactor Authentication, a hacker won’t be able to access his work data. Even if his phone is lost or stolen. Access is only granted when his identity is authenticated across two devices (i.e. phone and his laptop).
Like Jane, you may have a Joe in your life. Or several.

Protect yourself and your organization from them, with Optiv's help.

Take a look at more resources on our Cybersecurity Awareness Month Resources hub.

Get Started