Key Takeaways:
Cybersecurity Essentials for CPAs

Opkalla hosted a webinar for CPAs on keeping their firms cyber-secure. We interviewed Elliott Davis CIO, Jeff French, to hear his perspective on the current cybersecurity landscape, including how threats have changed over the years and the cybersecurity concerns that should be a top priority for CPAs to address. Read on to explore the key takeaways from the discussion.

On the current security and threat landscape and reason behind growth of attacks, both in size and quantity:

- There are many reasons for this growth:
  - Attacks are lucrative
    - Companies hit by ransomware attacks are increasingly willing to pay because doing so is cheaper than remediation.
  - Driving forces beyond money
    - Ego: “Let’s see if we can break into XYZ Company’s network, just to prove we can.”
    - Political: State sponsored attacks are extremely sophisticated. As we have seen in the media recently there have been some shocking revelations.
  - Barrier to entry is low
    - Ex. Tool kits to run an entire ransomware campaign can be purchased cheaply on the dark web. The tool kits are extremely easy to use and don't require a ton of knowledge.
    - Some countries are investing heavily in training their citizens to have a superb technical skillset but are not offering those individuals well-paying jobs to use those skills. Instead, the citizens use their skills as bad actors and commit cybercrimes for better pay and with less effort.
    - Vulnerabilities stemming from the human factor:
      - As we all know, humans are not perfect. Attackers know that too and prey on that fact. Very often the most compromises stem from not ultra-sophisticated tools, but people giving up their credentials willingly via an email with a link to a site that looks legitimate.

On the negative consequences of a data breach, including the less obvious ones:

- This is a big one. To put it bluntly - when faced with a breach or an attack, the literal survival of the company is on the line, depending on the severity or magnitude.
- In terms of the negative consequences, there are many:
  - Immediate and tangible effects of a breach:
    - Loss of revenue
    - Systems being shut down
    - Employees not being able to work/produce, etc.
  - The more intangible consequences are just as great:
    - The time it takes for remediation which encompasses:
      - Scoping the breach
      - Understanding the boundaries of the attack
        - What systems are affected?
        - What data was lost?
      - Restoring systems

            - Working with insurance carriers, law enforcement, legal teams
            - Notifying clients
        - Loss of trust and damage to reputation with both clients and employees
            - Loss of current and prospective clients
        - Potential for lawsuits
        - Breach at a CPA firm is more damaging to reputation than other industries
            - The CPA title implies that person should be trusted - it hurts more when that trust is lost

On the changing cybersecurity challenges at organizations like Elliott Davis (over the past 5 years):

- For IT one of the biggest challenges is staying on top of the emerging threats.
    - The last thing you want to happen is have your leader forward you a news article about a new vulnerability that you yourself hadn't even heard about yet.
    - Staying on top of all the new technologies, prevention methods, and compliance requirements.
        - The creation of new internal tools and client facing tools, without the traditional guard rails put in place by IT, has been a huge challenge here
    - In general, it's very difficult to filter through the noise and focus on what really matters
- Increased cybersecurity threats have required new actions:
    - Heightened access security – Elliott Davis has been enabling MFA for as many services as possible over the last several years
    - More services have been moved to the cloud
        - They've sacrificed some control for convenience and cost.
        - In some cases, these services are better positioned to protect their data than Elliott Davis was due to more sophisticated infrastructure. But - as we have seen in the media (looking back to the Solar Winds attacks or Log4J vulnerabilities), they know vendors are not impervious.
- Remote work has been challenging from a security standpoint:
    - Dealing with home networks and IOT devices, which are sometimes the absolute worst in terms of vulnerabilities
    - People trying to find their own solutions to new problems
    - People who still feel they need to print to do their job, creating a hard copy in an environment without secure shared facilities

On the most surprising challenges:

- The increasing amount of time IT teams must devote to cybersecurity
    - In the past security was usually somewhat of an afterthought - the focus was always on growth, capacity, speed, etc.
    - The increase in cyber threats and focus on security has created a $170 billion dollar a year industry. That number is up 30% in just 4 years. Incredible.
- Risks associated with the rise of the citizen developer
    - Tools are now so accessible to anyone with a credit card – they can go out and spin up enterprise class services without any guidance required from IT or some form of traditional governance
    - The barrier to entry is astoundingly low

On the cybersecurity concerns that should be a top priority for CPAs to address:

- From a compliance perspective, the ever-evolving regulatory landscape related to data handling
    - This can vary widely from state to state

  - Very difficult to stay current
- The human element
  - Humans are typically the first line of defense
  - Implementing an annual Security Awareness training is critical
    - Need to help people develop healthy skepticism regarding digital communication
- Rising of laptop theft
  - Protecting laptops will ensure data stored on them is not compromised
  - Having good backups is key too
- You can target these concerns by implementing a variety of systems and tools:
  - Email encryption
  - Drive encryption
  - A retention policy to delete old data
  - Segmentation to make sure employees only have access to the data they need access to
  - Regular Vulnerability assessments/penetration testing
  - Cyber audits of key systems
  - A response plan
    - Who is going to be your first call?
      - Legal support?
      - Cyber Insurance carrier?

On wariness some people have for creating a strong cybersecurity strategy because of (1) assumptions that nothing will be effective enough to keep up with bad actors, (2) it being too expensive or too complicated, etc. – and how to address these concerns:

- People with these concerns are not alone
  - This is not something **anyone** can do alone.
  - It is not purely a function of IT - it must be a team effort across the organization
- To combat these concerns:
  - Attack the low hanging fruit first
  - Hire a cyber security consulting firm
  - Perform an audit on your cyber footprint
  - Make recommendations based on impact or severity

On maintaining strong cybersecurity at a CPA firm where there is not a designated IT department (and there are many):

- Get good advice from experts
- Designate someone to oversee the security program and solution providers (can hire a fractional CISO, for example)
- Engage with security providers
- Ensure your contracts do not cause you to over-assume risk

On deciding when to build a security defense in-house vs. outsourcing to a cybersecurity partner:

- More and more [Elliott Davis is] moving towards a model of outsourcing to vendors who can perform round the clock monitoring of security platforms
- Occasionally certain platforms make more sense for them to manage in-house
  - This includes configuring and monitoring on their own.

On steps CPAs can and should take right now to protect their firms:

- Look at what is available to you through your current applications and security suite
    - See if apps offer some sort of MFA or additional security measures for login
    - Make sure you are taking advantage of all security features offered through your productivity suite
        - (i.e., Microsoft, G Suite, etc.)
    - See if your current security suite offers products that aren't being leveraged.
        - E.g., web filtering
- Ask your IT solutions provider what they recommend
    - If they can’t help, ask them to make a recommendation for a security solutions provider
    - It never hurts to have a fresh set of eyes on your environment to see what someone else might have missed