Cybersecurity: What you don't know can hurt you

In the 2020 SolarWinds attack, SolarWinds was unknowingly sending out software updates with code that created a "back door" to the very IT systems it had been hired to protect.

Information continues to be revealed about the scope and length of the SolarWinds attack, even as new attacks persist.

In the midst of these known cyber risks, the COVID-19 pandemic forced many institutions to quickly create processes to allow employees to work from home. Risk to data files, emails and systems—now being accessed outside of workplace walls and sometimes via employees' personal devices—increased exponentially. Unfortunately, sensitive information held by universities and hospitals makes them prime targets for cyber criminals.

This was proven in December 2020 and January 2021 when file transfer software provided by Accellion was compromised and data files with personal information from several universities were made available to download on a website run by cybercriminals.

Many institutions are now considering longer-term plans to allow for remote work, or at least be able to do so at a moment's notice. Diligent cybersecurity has never been so critical to thwart the efforts of criminals taking advantage of a crisis.

Assets and personal data associated with institutional retirement plans makes them especially tempting targets. On April 14 the DOL further emphasized the need for diligence in guidance released on cybersecurity program best practices for retirement plan sponsors, plan fiduciaries, recordkeepers and plan participants.

With increased flexibility comes increased risk

In 2020 those who could work remotely did. The FBI's Internet Crime Complaint Center (IC3) received a record 791,790 complaints from the American public (up 69% from 2019), with over $4.1 billion in reported losses. Business email compromise (BEC), phishing scams and ransomware incidents were most prevalent.

- **19,369 BEC scheme[1] complaints** with approximated $1.8 billion in adjusted loss
- **241,342 phishing scam[2] complaints** with $54 million+ in adjusted losses
- **2,474 ransomware incidents reported[3]**
  - Cybersecurity company BlueVoyant reported ransomware attacks on colleges doubled between 2019 and 2020.
  - New research from Check Point indicates the frequency of daily ransomware attacks increased 50% during the third quarter of 2020 from the first half of the year, with the U.S. healthcare sector the most targeted globally.

A report from email security firm Tessian looks at the state of data loss in organizations and reveals that nearly half of employees (48%) are less likely to follow safe data practices when working from home.[4]

Tips to help protect institutions

Build cyber safety into organizational culture and include a phishing awareness program
Institutions with a phishing awareness program are able to lower their susceptibility from the industry average of a 20% click rate.

Leverage two-factor authentication when administering financial plans and on all personal accounts
Even if a cybercriminal obtained your username and password, they wouldn't be able to complete two-factor authentication without access to your phone or secondary authentication device.

Practice least privilege when assigning access rights to institutional administration portals
Only give the amount of access the administrator needs to do the functions required of their role. The fewer individuals with access to sensitive data, the more secure the institution will be.

Keep all device security patches up-to-date
Regularly patching software and operating systems with up-to-date security fixes, prevents easy entry for intruders. This is true of personal devices, like phones and tablets, as well.

Share cyber safety education materials with participants
TIAA offers cyber safety flyers that can be shared with participants on topics like phishing, customer protection and authentication.

> **"By any measure, 2020 was the worst year ever when it comes to ransomware and related extortion events. And if we don't break the back of this cycle, a problem that's already bad is going to get worse."**
>
> — **John Carlin**, Acting Deputy Attorney General, on the U.S. Justice Department's newly formed task force to fight ransomware attacks

Take advantage of TIAA expertise

TIAA takes its responsibility for the financial futures of plan participants seriously and has long committed to maximizing the security of the information we maintain. Our global 24/7 security operations center monitors nearly 2 billion network events daily. Of those, we block or further review over 14 million events per quarter.

We were closely following the DOL's considerations on cyber guidance for plan sponsors, plan fiduciaries, recordkeepers and plan participants before it was released. We ensure compliance with what is outlined as strong service provider cybersecurity practices and have resources on our PlanFocus website to help both plan sponsors and participants stay safe.

These cybersecurity practices include:

- Following recognized security standards
- Outside auditor review and validation of security practices
- Transparency regarding security track record and past breaches
- Insurance policies that would cover losses
- Ongoing compliance with cyber and information security standards
- Contract provisions that cover:
  - Information security reporting
  - Use and sharing of information and confidentiality
  - Notification process for cyber breaches
  - Compliance with record retention and destruction, privacy and info security laws
  - Insurance

Click here for an overview of the security measures we have in place, and reach out to your TIAA contact if you're interested in hearing from one of our experts about ways to increase privacy and security for participants and institutions.

TIAA also has a wealth of information that can help employees protect their personal information and financial accounts. Visit the TIAA Security Center for tips on security when working from home, recognizing phishing and fraud, protecting elders from scams, and more.

Please reach out to your TIAA contact or the Administrator Telephone Center at **888-842-7782**, weekdays, 8 a.m. to 8 p.m. (ET) if you have any questions.

1. Federal Bureau of Investigation Internet Crime Complaint Center 2020 Internet Crime Report.
2. Federal Bureau of Investigation Internet Crime Complaint Center 2020 Internet Crime Report.
3. BlueVoyant Cybersecurity in Higher Education report, February 21, 2021.
4. May 28, 2020, report from email security firm Tessian.

1628370