BeneSys™ Navigator

TECH NEWS

Follow these clean desktop best practices to keep sensitive information safe

A clear desk policy requires employees to keep their workstations free of sensitive documents and information when not in use, including passwords.

Maintaining a clean desktop environment is an essential part of preventing cybersecurity events in any company, business or nonprofit. Clean desktops help protect sensitive information, prevent unauthorized access and reduce the risk of data breaches. BeneSys takes such protections very seriously and follows the best practices outlined below, some of which you may wish to consider using in your organization.

SHUTTERSTOCK.COM

- **Clear desk policy:** Implement a clear desk policy that requires employees to keep their workstations free of sensitive documents and information when not in use, including passwords.
- **Employee awareness training:** Conduct regular cybersecurity awareness training sessions to educate employees about potential threats, phishing attacks and social engineering techniques.
- **Secure document disposal:** Encourage employees to shred or otherwise properly dispose of sensitive documents, both physical and digital, when they are no longer needed.
- **Screen locking:** Enforce the use of automatic screen locking after a period of inactivity to prevent unauthorized access to a user's workstation. Our employee training teaches BeneSys staffers that anytime they walk away, they must lock their workstations.
- **Secure workstation lockdown:** Regularly update and patch operating systems and software to prevent vulnerabilities that could be exploited by cyber attackers.
- **User privilege management:** Limit user privileges to only what is necessary for each job role. Limiting and monitoring user privileges helps prevent unauthorized access to critical systems and data.
- **Password policies:** Enforce strong password policies, including regular password changes and the use of multifactor authentication for access to sensitive systems.
- **Secure storage of removable media:** Control the use of USB drives and other removable media, and restrict their usage to prevent data leakage and potential malware infections.
- **Endpoint protection:** Install and maintain up-to-date endpoint protection software, including antivirus and antimalware solutions, on all workstations.
- **Regular security audits:** Perform periodic security audits to assess the cleanliness of the desktop environment.

Remember that maintaining security is an ongoing process, and everyone in the organization is responsible for it, so regular assessments and updates are crucial to stay ahead of potential threats. ●

FROM THE CEO

Labor of love

“Thanks to all those in organized labor for everything that you do to help make lives better for your families and all Americans.”

by Ed Wolyniec, CEO

We typically publish the Q3 issue of *Navigator* in early September, so Happy Labor Day! If you’ve read my *Navigator* column in past years, you may know that this issue is when I usually like to do two things:

1. Say thanks to all those in organized labor for everything that you do to help make lives better for your families and all Americans by delivering a solid day’s work in exchange for fair pay and benefits. This drives the middle class!

2. Find a fact or two, preferably obscure or maybe a little strange, related to Labor Day — perhaps about the holiday’s origins or how America celebrates it. Here goes:

Labor Day, according to *Reader’s Digest*, is tied with Memorial Day as the second most popular U.S. holiday for outdoor grilling (July 4 holds the top spot). An interesting article in *Good Housekeeping* noted that the sale of hot dogs drops dramatically after Labor Day and the end of the traditional grilling season. And finally, for a related/unrelated fun fact, Labor Day will truly be a day of labor for the 11,000 or so women who will give birth on that day.

Thanks for reading, and please know that we really appreciate being your third-party administrator and software solution provider. We’re proud to support your trust funds and your members! •

Recognizing exceptional BeneSys employees

EMPLOYEE SPOTLIGHT: Nicole Quinn, member services

Who: Nicole Quinn, member services representative in our Troy, Michigan, office.

Why she stands out: She’s a repeat recipient of our quarterly Service Excellence awards, nominated by her peers.

History at BeneSys: Nicole joined in 1999 (24 years and counting), and worked in contributions and claims before moving to member services.

Advice for others working in the Taft-Hartley benefit space: “Even though it’s a lot of work and a lot of information to learn, just stay humble and don’t give up.”

Hobbies outside of work: Baking and spending time with friends and family.

A word from her boss: “Nicole’s resilience, dedication and positive attitude are inspiring!” says Becka Mundy, member services supervisor. “Nicole faces challenging situations head-on and strives for resolution for our members. It is wonderful to work alongside someone with such wisdom and experience!”

COMPLIANCE

Labor Department offers 8 tips for protecting retirement savings online

by Tom Shaevsky, General Counsel

Tom Shaevsky is general counsel at BeneSys Inc. He has spent nearly 25 years practicing ERISA/employee benefits law.

The U.S. Department of Labor recently issued reader-friendly information reminding the public to protect electronic data.

In her blog post "8 Tips for Protecting Your Retirement Savings Online," Assistant Secretary of Labor for Employee Benefits Security Lisa M. Gomez suggested the following to help reduce the risk of fraud and loss to an individual's retirement account:

- **Monitor your online account(s) regularly.** Checking your retirement account(s) periodically reduces the risk of fraudulent access and allows you to identify any suspicious activity.
- **Use a strong and unique account password.** Avoid using dictionary words, sharing passwords or repeating passwords for your online retirement account. Instead, use a long password containing a mix of letters, numbers and special characters. Update your password regularly.
- **Use multifactor authentication.** Logging in to your account may require more than just your username and password. You might be asked to verify your identity by using a fingerprint or entering a code sent by email or text. While multifactor authentication might seem inconvenient, it can be a very effective way to prevent an unauthorized person from accessing your account. (See "Multifactor Authentication Matters" at left.)
- **Keep account and personal information up to date.** Update your contact information whenever it changes. Close unused accounts.
- **Be cautious about free Wi-Fi.** When checking your retirement account, avoid using a public Wi-Fi network, which can easily be accessed by criminals. Instead, use your cellphone for internet access if you are away from home.
- **Beware of phishing scams.** Phishing attacks often target your passwords, account numbers and sensitive information in order to access your accounts. A phishing message may appear to be from a trusted organization to lure you into clicking on a link. Warning signs include unexpected text messages or emails, especially those that contain spelling errors or poor grammar.
- **Install antivirus software, and keep your apps and software up to date.** Outdated software and applications can be a security risk. Use trustworthy antivirus software, and keep it and other software updated with the latest patches and upgrades.
- **Report identity theft and cybersecurity incidents.** If you are a victim of a cybersecurity attack, file a report with the FBI at www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view or with the Department of Homeland Security at www.cisa.gov/report. •

This article is provided for informational purposes only and does not constitute legal advice. Readers should consult with their own legal counsel before acting on any of the information presented.

Multifactor authentication matters

In a recent cybersecurity newsletter devoted to the topic of authentication, the U.S. Department of Health and Human Services reiterated many of the key points we shared with you in our Q1 2023 *BeneSys Navigator* cover story, "Multifactor Authentication Means More Than Just Strong Passwords." HHS noted that while weak or nonexistent authentication processes leave electronic information open to intrusion by malicious actors and increase the likelihood of potential compromise of sensitive information, "stronger authentication processes can impede or prevent many cyber attacks — especially attacks that rely on the use of weak or stolen passwords."

For more information about multifactor authentication — what it is, why it's important and how we use it at BeneSys — download our Q1 2023 issue at benesys.com/wp-content/uploads/2023/03/BeneSysNavigatorQ1_2023.pdf.

Fraudsters rely on too much trust, too little verification

by Lee Centrone, Senior Vice President

BeneSys Senior Vice President Lee Centrone has been a trust administrator for more than 20 years, working with trust funds from many industries.

Kickbacks, cooking the books, identity theft — the threat of fraud looms large these days, and mitigating it is a key fiduciary responsibility for benefit plan trustees. Fraud happens when someone has a motive to commit the crime, rationalizes their actions and takes advantage of the opportunity to defraud. Trustees can't control the motives or rationalization of a fraudster, but they can reduce the opportunity.

Opportunities for fraud

Fraud is costly and happens when there is too much trust and too little verification. It can be committed by any number of people — from plan professionals and their employees to trustees, Participants, medical providers and outside bad actors. Fraudsters may attempt to take advantage of a trust fund's assets and data in a variety ways:

- **Contributions.** Examples include employers "hiding" employees to avoid paying the contributions due, purposefully failing to report on all hours due, or reporting contributions on extra persons in order to add them to the health plan.
- **Investments.** Examples include stealing securities or cash, not receiving all income due on investments held, understating sales proceeds, inflating market valuation, or not receiving stock splits and dividends.
- **Benefit payments.** Medical benefit examples include billing for services never performed or submitting bogus health claims. Pension benefit examples include cashing benefits for deceased pensioners or submitting false direct deposit change forms for retirees.
- **Expense payments.** Examples include inflating professional fees or expenses, or using the fund to pay personal expenses.

Mitigating the risk

In our role as plan administrator, BeneSys uses many best practices to help our employees as well as the trustees we serve mitigate the risk of fraud. These best practices include:

- **Division of duties.** We provide checks and balances by engaging multiple people in certain activities. For example, three people are involved in the process of paying an invoice, and a minimum of two people review every pension application.
- **Clean, current data.** We work to keep your Participant data clean to minimize the number of missing Participants and to quickly learn of any deaths.
- **Timely, accurate financials.** We make sure that each trust's monthly financial statements are completed in a timely manner and that bank reconciliations are completed by the appropriate people.
- **Controlled contributions.** To combat fraud in trust contributions, our system is set up according to the relevant collective bargaining agreement and provides tight administration of each trust's payroll audit and collection program.
- **Routine reporting.** To mitigate the opportunity for fraud (or just error) in trustee reimbursements, we follow your plan policy and recommend distributing reimbursement reports at trust meetings.

At BeneSys, protecting trust assets and data is central to the role we play in every plan. If you have any questions about fraud mitigation, please ask your plan manager. •

EXPANSION

2 years strong: BeneSys and Beacon celebrate a growing partnership

SPYGLASS

SpyGlass, our enterprise-class health claims management software, offers a powerful, flexible solution for precise and timely claims processing. SpyGlass makes benefit and plan setup remarkably straightforward.

LEARN MORE

To learn about Beacon products and solutions, including SpyGlass, visit beaconspyglass.com. To learn about BenefitDriven, visit benesys.com/technology /benefitdriven.

June marked the two-year anniversary of BeneSys acquiring Beacon Technologies Group and, we're delighted to report, both companies are still feeling the glow.

"Beacon continues to grow and cement its position as an industry leader in providing health claims management technology solutions, bringing benefits to both Beacon and BeneSys clients," says BeneSys CEO Ed Wolyniec.

"Probably the most visible change is the integration of BeneSys' BenefitDriven technology into our SpyGlass software," says Beacon CEO Ernie Crawford. "Together we've delivered a comprehensive benefit administration solution offering for the Taft-Hartley market."

That's one of many changes that Beacon, which has been building solutions for health claims management since 1995, has made in the past 24 months. The company has also:

- **Enhanced** its suite of health claims management applications.
- **Increased** its research and development efforts.
- **Accelerated** the growth of product innovation.
- **Expanded** its presence in the marketplace.
- **Strengthened** its infrastructure.

In addition, Beacon continues to invest in its team. "In order to support our growing initiatives and with our clients top of mind, we've expanded our workforce by nearly 40%," says Ernie. "We have added development, business analyst and quality assurance resources."

The company also expanded an in-house conversion factory team, which is wholly dedicated to getting new clients up and running smoothly.

"We're proud of everything we've accomplished in the past two years," Ernie says. "We sincerely thank the BeneSys team and our clients, partners and employees for the role they've played in these successes."

"When we acquired Beacon, we saw it as an investment in enhancing BeneSys' core competencies and improving our client service," Ed says. "We've been able to deliver great new technology to existing BeneSys clients, so clearly our investment is paying off. We look forward to all that our partnership with Beacon has in store in the next two years and beyond." •

ABOUT BENESYS

BeneSys has been providing Taft-Hartley trust fund administration and IT services since 1979. Our dedicated specialists understand the nuances of Taft-Hartley benefit plans, and our software system, BenefitDriven, is designed to give our clients and their plan Participants the most efficient tools for self-administering trust fund accounts.

CORPORATE & OPERATIONAL HEADQUARTERS
700 Tower Drive, Suite 300
Troy, MI 48098-2808
248-813-9800

WEST COAST HEADQUARTERS
7180 Koll Center Parkway, Suite 200
Pleasanton, CA 94566-3184
925-398-7060

BUSINESS DEVELOPMENT
National Sales Director
Thomas Lally: 401-378-1299
thomas.lally@benesys.com

SaaS Inquiries
Blake Holderread: 217-801-8911
bholderread@beaconspyglass.com

www.BeneSys.com

FOLLOW US
To keep up with BeneSys
between *Navigator* editions,
visit us at www.BeneSys.com
or follow us on LinkedIn.