

# VENDOR MANAGEMENT PLAN

*Meet compliance requirements, reduce security risks*

By Jay Mallory, ImageQuest Executive Vice President, Marketing & Business Development

**So, you've done some serious tightening up of your IT Security.**

You closed-up some gaps, trained your workers to delete phishing emails, and you have some robust IT security systems now in place.

Great! But what about your vendors who access your business records or IT systems? Is their IT Security as tight as yours?

Regulators are very aware that a lot of breaches start with a vendor. The Ponemon Institute put it as high as 61 percent of breaches.

Hackers know this too and often will try to penetrate the weaker security of the smaller downstream vendor.

The 2014 Target breach is a classic example of this. Target had strong security – but the HVAC

*continued on P.02*

*Your vendors often access business records online. Is their IT Security as tight as yours? Hackers know this and can try to penetrate the weaker security of a*  
**DOWNSTREAM VENDOR.**



**IN THIS ISSUE:**

- P.02** Team News
- P.03** From Our Blog
- P.03** Meet A Cyber Criminal
- P.04** Welcome New Client
- P.04** Client Comments

*Milton Bartley*



*Jay Mallory*



**IMAGEQUEST**

**Your Managed IT, Cybersecurity & IT Compliance Experts**

*continued from P.01*

vendor accessing its network did not. As a result, malware installed on the HVAC's company's systems made an easy leap onto Target's systems.

Even the latest breach in the news – of Capital One data on the Amazon Cloud Service – has vendor implications. Amazon says its systems worked correctly and the breach occurred because Capital One failed to configure some security software correctly.

It's been an embarrassment to Capital One, whose CEO said this spring that Capital One was "a technology company that does banking." Some observers have questioned whether Amazon has some responsibilities there too.

So, while you may be cutting edge with your IT Security, the third-party or vendor organizations, your company works with could leave you vulnerable. Examples could include vendors who handle your billing, your collections, your payroll, your HR, your legal work, your IT, or even your building systems management and security.

If you are one of those downstream vendors, your security will come under scrutiny. Your clients will want to know how secure their data is as it progresses from creation to disposal. And if you are an organization with Personally Identifiable Information or Intellectual Property, your regulators are probably already raising this issue with you.

In either case, a Vendor Management Plan will come into play.

A vendor management plan is a document that details how you risk rate your vendors. That risk rating will depend on how critical the services that vendor provides are to your overall business, and what access that vendor has to your IT systems or data.

***If you are a downstream vendor, your security will come under scrutiny. Your clients will want to know how secure their data is.***

A well-written and managed vendor management plan can help you determine whether the vendors that access, transmit, store, or dispose of data from your organization meet the appropriate regulations and use appropriate security measures.

Businesses and organizations operating in highly regulated industries may be required to closely monitor their vendors and third-party providers for compliance issues. In some sectors, NOT effectively managing vendors may lead to fines or penalties.

Here's an example:

Let's say you provide medical billing services or utilization review and need access to St. Local County Hospital's electronic medical records system.

The hospital may have millions of electronic health records (ePHI.) It has invested significant money to keep those records in compliance with regulatory requirements. And those regulatory requirements will include the need for due diligence of vendor data security measures.

So, if your utilization review company needs access to hospital medical records to provide service, you will have to sign a Business Associate agreement obligating your company to use "appropriate safeguards" in handling the ePHI – and to follow regulatory requirements around breach notification.

You also have to require your subcontractors handling that data to do the same.

A vendor management plan is crucial in today's regulated marketplace. It can be an extensive process, and we can help with it. Start by learning more with our current White Paper at <https://www.imagequest.com/white-papers/>.

## TEAM NEWS

Our interns have headed back to school, but we've welcomed two more hires to the ImageQuest team.

**AMY PFEFFER** has joined us as a senior client relationship manager. She previously worked at Premise Health in Nashville as Manager, Technology Project Management.

At Premise Health, Amy oversaw the installation of technology. Her experience includes establishing



AMY PFEFFER

Epic electronic medical records and patient portal systems at onsite employee health clinics Premise built for 370 clients, including Disney, Intel, Microsoft, and BMW. The Epic rollout by Premise Health was one of the

fastest in Epic's history.

In her new role, Amy says she looks forward to helping clients meet their business needs with solutions developed by ImageQuest's technology experts.

"I want to really know who each client is along with where they envision themselves from a business strategy," she says. "I want to ensure they feel they have a partner and someone with their vested interests at heart."

**JAMESON FITZGERALD** has joined us as an IT Support Specialist II. His background includes experience as a help desk analyst for UPMC (University of Pittsburgh Medical Center), an Application Support Analyst for Aetna, and Help Desk Support for Aethon.

Jameson is a "huge" Pittsburgh Steelers fan and had a stint as a ball boy for the Steelers in 1998.

But he is originally from Nashville and recently moved back from Pittsburgh to be with family.

# FROM THE IQ BLOG:

## Preparation for data breach can save \$1.2 million

A recent study by IBM and the Ponemon Institute shows the costs of data breaches continue to rise, in part because of increased regulation and “the complex process of resolving criminal attacks.”

The study found breaches hit small and midsize businesses rather hard, with the average loss due to a breach costing more than \$2.5 million on average. Healthcare breaches were the most expensive, and U.S. breaches cost twice as much as breaches elsewhere in the world.

However, companies that had both prepared for a breach and tested their plans saved themselves \$1.23 million in breach costs. Also, companies able to detect and contain a breach in less than 200 days saved \$1.2 million in recovery costs.

The most common reason for a breach was a “malicious cyberattack,” the study said.

### COST OF BREACHES

Additional factors impacting the cost of a breach for companies in the study included:

- Data breaches cost companies around \$150 per record that was lost or stolen.
- Using security automation technologies, such as those used in managed detection and response cut the average cost of a breach in half, from \$5.16 million to \$2.65 million.
- Third-party breaches— such as a vendor or supplier – cost companies \$370,000 more than average. Companies need to closely vet the security of the companies they do business with, make sure their security standards align, and actively monitor third-party access.

— <https://bit.ly/IQBlog072519>

31.012

## MEET A CYBERCRIMINAL

Meet **EDUARD MALANICI**, 32, of Balti, Moldova.

The U.S. Department of Justice says he ran a crypting services operation called “procryptgroup” for cybercriminals in 2016. The feds suggested in an indictment that he may have advertised his services on “underground, Russian-speaking, online criminal forums, including Mazafaka, Verified, and DirectConnection.”

His customers were distributing the GozNym malware, a banking trojan, and needed his help in hiding the malware from most antivirus programs.

According to security blogger Brian Krebs, a crypting service scans a piece of



EDUARD MALANICI

malware against all available antivirus tools to see how many of them detect the malware. The service then runs encryption to “obfuscate the malware.” The malware no longer resembles any malware definition held by the antivirus programs – and thus can’t be detected.

GozNym was installed on victims’ systems through

phishing emails disguised as invoices delivered from Intuit, QuickBooks and other programs.

The invoices demanded payment at fake websites that looked like a website called “billpay-center.com.” However the actual address began as “hXXp://” instead of the usual “https://”.

GozNym also used a keystroke logger to steal login credentials to steal funds from the bank accounts of small businesses in the U.S.

Victims included law firms, which lost more than \$117,000; an electrical device supplier, which lost nearly \$200,000; a medical equipment company which lost nearly \$99,000; and a paving company that lost more than \$121,000. There were many more victim businesses – but the attempts to steal up thousands of dollars from their bank accounts were blocked.

The Justice Department indicted ten people, primarily from the region around the Black Sea, as co-conspirators and contributors in the conspiracy. Half of them, including Malanici, were arrested. The other five remain free in Russia, according to the FBI’s Cyber Most Wanted.

### DO YOU KNOW A COMPANY LOOKING FOR IT SUPPORT?

#### WHAT WOULD MAKE A GOOD REFERRAL?

A great referral for us is a company in any professional industry with at least 20 computers – or any organization with a regulatory compliance standard they must follow.

#### HOW DO I SUBMIT A LEAD?

You can submit your referral by emailing us at [leads@imagequest.com](mailto:leads@imagequest.com), or by calling Milton Bartley or Jay Mallory at 888.979.2679. You can get more details at <https://www.imagequest.com/referral-program/>

I recommend  
**IMAGEQUEST**  
for their Expert IT Service

# WELCOME NEW CLIENT!

**Sunrise Services helps small, independent medical practices get paid for their services. Specifically, Sunrise helps primary care and behavioral health doctors with billing and revenue collection and electronic medical records maintenance.**

"We're the back office working to keep (the medical practice's) revenue coming in," said Kelly Meeks, President of Sunrise Services. "We work to keep the doctor from pulling his or her hair out over this regulation and that metric. We help with all of it."

Sunrise started 22 years ago as a medical billing firm. Meeks said initial services included certified coding work to make sure doctors' invoices contained the correct coding on patient progress. As medical records have evolved to Electronic Medical Records (EMR,) the need to assist with coding has declined. But other services have grown in billing, statement processing, electronic claims help desk support has grown.

"I always say I have a super exciting job reading government regulations for doing medical billing. I love it," Meeks said. "But I'm super passionate about this. I want the doctor

to be paid. I believe they deserve payment for their services just like everyone else."

Sunrise came to ImageQuest after realizing that it was falling behind in meeting compliance regulations, particularly for HIPAA. Meeks said the company discovered several gaps with a previous IT provider.

Meeks said she then met Jay Mallory, ImageQuest's Executive Vice President for Business Development and Marketing, at an event hosted by The Chamber Jeffersontown.

"I really liked talking with him," Meeks said. "Jay knew what he was talking about in the healthcare space and was very patient in answering questions."

Ultimately, ImageQuest moved Sunrise's IT infrastructure to a secure and compliant data center and is providing ongoing IT management and support.

"I feel very confident in their ability to keep me compliant," Meeks said. "We host EMRs, we host billings services – so there are other mouths at stake. It's not just my company. I preach 'hire out your deficiency, the things you're not good at. Find somebody where that's all they do, and they're good at it.'

"I preach that to my clients, and I should follow my own advice, right?" 🗣️

## Check Us Out!

### OUR LIVE EVENTS

**Aug. 25-26**

Bluegrass Community Bankers' Assoc., Lexington

**Sept. 9**

Greater Louisville Assoc. of Health Underwriting, Louisville

**Sept. 21-25**

Kentucky Bankers Assoc. Convention, The Greenbrier, WV.

**Oct 7**

Nashville Non-Profit Technology Training, TechBridge TN, Nashville

## Follow Us

Look for us on Social Media to learn more about us and keep up with related news. Follow us on LinkedIn and Twitter. From time to time we add Video Tips on YouTube to help you stay secure. Due to data privacy concerns, we are not on Facebook.



### MEET SUNRISE SERVICES, LLC

**Location:** Mount Washington, KY

**Founded:** 1996

**Website:** www.sunrise.com

**Services:** Provides Revenue Cycle Management for small, independent Medical and Behavioral Medicine practices.

## From Our Customers

"My experience was great because Angie worked tirelessly to resolve the issue, even following up twice. Great service!"

"Erick was so helpful and patient. Thank you!!"

"The problem was fixed within 30 seconds, and I now know how to tackle it myself in the future!"

"Love the follow up on an issue that was not resolved by a different vendor."

"Thanks, Josh, for being prepared and executing timely!"

"Davis was able to remote into my laptop and discover the problem with my printer. He was kind, professional, and resolved my problem fairly quickly!"

"Thank you so much for the amazing customer service and attention to detail. You guys are awesome, and we are very grateful!"

"Damian was very helpful and got my connection fixed."

"The Help Desk was quick to return my call and followed up to ensure that the issue was resolved."

**Thank YOU to our clients who shared their positive feedback about our help. We appreciate it! If you are not having this experience with your Technology Vendor, maybe you should give us a call!**