



# AUDIT FATIGUE Q&A

More efficiently auditing cybersecurity and data privacy programs

## Abstract

Four experts in security and compliance, with broad experience in the public and private sectors, sat down together during the *Cyber Risk and Data Privacy Summit* hosted by *Compliance Week* to discuss the impact of the growing audit burden on IT organizations.

## Participants

### STEVE HORVATH

Vice President of Strategy and Cloud  
Telos Corporation

### PETER GOULDMANN

Enterprise Risk Officer for Cyber  
U.S. Department of State

### JEAN SCHAFER

President and CEO  
Verity Insights, LLC

### LANCE DUBSKY

Chief Security Officer  
Quintillion Subsea Operations, LLC





## TABLE OF CONTENTS

Introduction.....	3
Q: Does Audit Fatigue weaken security and privacy programs?.....	5
Peter Gouldmann .....	5
Lance Dubsky .....	6
Jean Schaffer .....	7
Q: How can operations, compliance, and risk management teams better cooperate?.....	8
Jean Schaffer .....	8
Lance Dubsky .....	8
Peter Gouldmann .....	9
Q: What unforeseen or unintended costs are caused by audit fatigue?.....	10
Lance Dubsky .....	11
Jean Schaffer .....	11
Peter Gouldmann .....	12
Q: What are the personnel costs of audit fatigue?.....	12
Peter Gouldmann .....	12
Jean Schaffer .....	13
Lance Dubsky .....	13
Q: Can automation relieve audit fatigue? .....	14
Lance Dubsky .....	14
Peter Gouldmann .....	15
Q: What would make internal audits more beneficial? .....	15
Q: How do you approach risk management of M&A?.....	16
Additional Resources .....	16

# AUDIT FATIGUE Q&A

## More efficiently auditing cybersecurity and data privacy programs

### INTRODUCTION

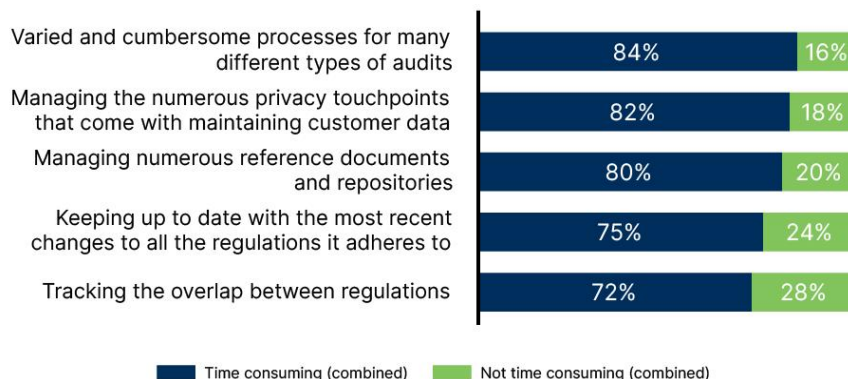
In the face of constantly increasing security and privacy standards, IT organizations struggle to hire and maintain staff with the experience and training necessary to meet compliance demands. In this day and age it's nearly impossible to be 100 percent compliant with all applicable standards. The personal, professional, and organizational repercussions of the growing strain of audit fatigue are real. Constant visits from auditors, both internal and external, can be daunting, bringing with them the potential for fines and damage to an organization's reputation.

Audit fatigue is not just expensive at the organizational level. Individual practitioners suffer low job satisfaction and job burnout.<sup>1</sup>



The most time consuming task security professionals face is managing the varied and cumbersome processes for the many different types of audits they face (84%).

Time consuming compliance tasks



Excerpted from *A Wake Up Call: The Harsh Reality of Audit Fatigue*

During a virtual event held during January 2021, the *Cyber Risk and Privacy Summit* hosted by *Compliance Week*, Telos Corporation's Steve Horvath hosted a panel discussion of the impact of audit fatigue featuring experts with rich experience in government and industry. Steve serves as Vice President of Strategy and Cloud, and has been doing risk management and compliance activities for over 20 years. At Telos, he works directly with senior security and compliance officers at many client organizations.

<sup>1</sup> Vanson Bourne for Telos Corporation, *A Wake Up Call: The Harsh Reality of Audit Fatigue*



Steve's guests during the panel discussion included:

**Jean Schaffer**, President and CEO of Verity Insights, LLC, a small consulting firm she



founded after retiring from the Intelligence Community. During her government career, Jean worked at both NSA and CIA for over 30 years, primarily focused in the security arena, as well as running the operational infrastructures for both agencies. She has a background as an authorizing official and risk manager and has managed 24/7 operations centers as well as compliance organizations.

**Lance Dubsky**, Chief Security Officer for Quintillion Subsea Operations, LLC. He began



his career with the U.S. Air Force. He then entered civil service, working for the Intelligence Community, including the National Reconnaissance Office and National Geospatial Intelligence Agency, as the Deputy Chief Information Security Officer, Authorizing Official, and person responsible for audit and compliance. Having retired from the government, he now works

for Quintillion, a leading provider of Gig-E broadband and ground station as a service in the U.S. Arctic.

**Peter Gouldmann**, Enterprise Risk Officer for Cyber and Director of the Global IT Risk Office, U.S. Department of State.<sup>2</sup> He started his cyber career



working very closely with the National Institute of Standards and Technology and the equivalent body in the national security space, working on many of the standards and guidelines that are used by auditors within the government to evaluate information security programs. Over the span of nearly two decades working in cybersecurity, he has been subject to annual audits and

inspections from the Government Accountability Office as well as the internal organization's inspector general.

Presented in this paper are the questions posed to the panelists during the January 2021 *Cyber Risk and Privacy Summit* and their various experiences and insights in response.

---

<sup>2</sup> Any views or opinions attributed to Mr. Gouldmann are his own and do not necessarily reflect those of the U. S. Department of State.



## Q: DOES AUDIT FATIGUE WEAKEN SECURITY AND PRIVACY PROGRAMS?

**Steve Horvath:** Each of you has been involved in multiple organizations with roles directly related to risk management and compliance activities, as authorizing officials, CISOs, CEOs, risk officers. In these roles, how have you seen audit fatigue weaken the programs or the privacy of the enterprise or its programs?

**Peter Gouldmann:** There are a couple of things in the federal space to bear in mind. Most of the cybersecurity audit activities today occur as they were set forth under the Federal Information Security Management Act (FISMA) of 2002. These audits have been happening for a very long time. From 2002 through 2014, there was a lot of controversy. Practitioners kept pointing out that there seemed to be some gap between what was being audited and the actions necessary to conduct effective cybersecurity operations. This at-odds perspective made organizations feel like that they weren't getting credit for the good work they were doing, which was fighting the cyber battle. On the other hand, they didn't feel they had the necessary resources in place and didn't fully understand how compliance with that law and its subsequent guidelines and regulations would improve their ability to operate in cyberspace.

In 2014, FISMA was rewritten. It retained the same letters, FISMA, but it became the Modernization Act as opposed to the Management Act. One of the principal changes among many was the striking out of compliance and replacing it with effectiveness, an attempt by the Congress to understand that effective security was more important than compliant security.

---

*Effective security is more important than compliant security.*

---

At the same time, auditors switched from doing an audit that was a compliance review to a maturity model; somewhat like the capability maturity model five-level approach. Initially, they faced the challenge of trying to figure out the differences between a compliance-based or evidence-based approach to auditing and what would be the right way of approaching from a security effectiveness perspective. They've been plagued in the past with issues like, "if I've done some things at a level three but most of the things are at a level two, am I at a two-plus or am I at level two? Do I have to do everything at one level before the next?"

With that as a backdrop – the challenges from a practitioner's perspective of the dichotomy of program effectiveness versus cyber operations effectiveness – most organizations have struggled to resource and address both the regulatory requirements



through the audit practices and the cyber operations activities that the agency feels necessary to keep themselves protected and assure their operations.

That in addition the audit cycle itself, which frequently takes multiple months for an audit to be conducted, starting usually in the March/April timeframe and concluding in October or November, leaves very little time in the cycle to actually work on improvements before you're producing evidence for the next cycle of audit. So by no means is it a perfect environment, but I can't point fingers at a failure that somebody's set up on purpose. It is just the consequence of the events.

So on one side, you've got a number of people working hard to perform cyber operations and on the other side, you have that churn and constant oversight activities. You can't ignore one for the other. There's a famous line from a movie years ago called *The Right Stuff*. When the astronauts asked Wernher von Braun what makes rockets go up, he said, "Fuel." They said, "No. Funding." So you get funding because you're meeting regulatory requirements and if you're meeting requirements, you're drawing resources away from the cyber operational activities, or at least it appears that way. That's the challenge we face.

---

*You get funding because you're meeting regulatory requirements and if you're meeting requirements, you're drawing resources away from the cyber operational activities.*

---

**Lance Dubsky:** At a couple of the companies that I've worked with over the past five or six years, one of the challenges is that when you're a publicly traded company, and when you have compliance oversight that could impact revenue, you have to satisfy your board of directors with the right kind of a compliance approach. Coming from the government side, I typically had a lot more money to do risk management well and to build systems right. The result of that typically is good compliance – if you build things the right way, you typically are compliant. Even if they're not compliant, you can show evidence that you have secure systems because they were built right.

On the commercial side, the challenge is a bit bigger because you have some additional requirements. When I worked for a real estate investment trust (REIT), we had 226,000 customers, including 95 percent of the Fortune 1000, and held a lot of very sensitive data including financials. When you have the FDIC, the OCC, and the Federal Reserve Bank coming in looking at your program, it's different than the government method. Rather, every month you're having to brief some state of compliance to external auditors and the board. When you're trying to meet compliance so heavily, it basically takes all of your manpower away from building security into your new systems and applications. It's kind of a painful double-edged sword.



So what do you do? You typically have a lot of long hours. It's not a 40-hour a week job; it's sometimes a 60- or 70-hour a week job. You definitely see the audit fatigue when you're trying to figure out, "How am I going to put together the right kind of information to brief all of the different auditors?" You may even have to rank audits according to which one is going to impact revenue most if you don't deliver.

---

*You may even have to rank audits according to which one is going to impact revenue most if you don't deliver.*

---

It can especially be a challenge if you're used to building risk management programs a particular way, with information security professionals, security engineers, risk management, and testing people. And they're all doing the right thing to build secure systems. When you do it that way, it seems like the outcome automatically is that you get good compliance. But in some of the situations I faced, that was not yet established, and the board had a mandate that you need to deliver a particular level of compliance.

One particular thing I had to deal with was related to vulnerabilities. I was told, "You have a million vulnerabilities to work down between now and the end of the year." And after I used the right set of tools, I discovered it wasn't a million. It was more like four million, and was growing by a hundred thousand every month.

So all of a sudden you start looking at your tools such as BigFix, LANDesk, and all of your automated patching tools, to make sure they are set up the right way. No matter what kind of vulnerability system you're using, all of those tools make a big difference.

You definitely see audit fatigue in the commercial sector when you're trying to comply with so many different audits.

**Jean Schaffer:** I would echo what Peter said earlier. I remember those early days when we were still arguing about what question we were actually trying to answer. It has improved over the years, but the big take away, at least from the government side, is we truly did try to focus on doing the right thing. If you build security into your products, if you focus on doing good cybersecurity, then the auditing is almost a second thought. If you have done things the correct way, the audits and the compliance are just the evidence to prove that you have done that.

---

*When it's time to meet the various audits and the compliance checks, we should be automated enough to be able to pull out those results and prove where we are on that scale.*

---

That is a perfect, idealistic world. I will tell you, everyone still struggles. None of us is there yet. The goal that most of the Intelligence Community adheres to is to build and



protect and configure all of our IT in the proper way. When it's time to meet the various audits and the compliance checks, we should be automated enough to be able to pull out those results and prove where we are on that scale.

## Q: HOW CAN OPERATIONS, COMPLIANCE, AND RISK MANAGEMENT TEAMS BETTER COOPERATE?

**Steve Horvath:** While security is everyone's responsibility, personnel in security operations, compliance teams, and risk management personnel need to work together to form a logically cohesive unit to combat threats. Often, these activities feel like fighting a losing battle and the outcomes hinder necessary relationships. How can the partnership and flow of communications be maintained among these important teams?

**Jean Schaffer:** For any program, it is really important to agree up front on the sources of compliance records. You are talking about three different groups. They may or may not report to the same manager. If you go to each of those groups and ask for something even as simple as the number of assets on the network, depending on what tools each of those groups relies upon, you'll get a different answer every time. You don't get the consistency of information that you need to tackle whatever compliance or security issue you're having.

---

*Depending on what tools each of those groups relies upon, you'll get a different answer every time.*

---

From the get-go, you need to lay out clearly the system sources of record and the tools to gather the compliance data each time that you have to answer a question. Consistency among the groups is a really big thing. When you have different organizations giving different answers, it turns into finger pointing, or "Mine's better than yours," or "How come yours is missing something?" So clarifying that framework up front – what data are you gathering and how are you gathering it – would be my advice.

**Lance Dubsky:** This is a challenge on the commercial side even more than on the government side. On the government side, we were able to do a pretty comprehensive inventory and put everything into a particular database. So we had a really good record. But on the commercial side, we did not have a complete asset inventory. So we brought in a third party vendor to do a comprehensive asset inventory and to populate everything into ServiceNow. That enabled us to validate with all of the system and data owners, and then define the business critical systems with data owners. That is really important because if you don't know what those are, then you have no idea how to apply vulnerability management, threat management, and all of those other things to





what's critical. If you haven't defined that, then everything is equal. That inventory enabled us to define those business-critical systems and applications so that when we were tackling compliance, we were focused heavily on the business-critical side.

Trying to get technology, application owners, and security to work together is one of the greatest stresses. Working with the different data owners can be a challenge. In that particular company they were senior vice presidents. I was a vice president, but I worked for an executive vice president who was the boss over all of these individuals. My boss had given me the mandate to increase staff accountability on what needed to be done and report back, which is a fantastic scenario if you're that fortunate. So we were able to get a lot of leaders and functions on board with defining what those important assets were and what needed to be audited. It doesn't mean that the audits went well. It doesn't mean that there weren't a lot of gaps in reporting on compliance. In addition, the company had outsourced most of the IT, which added another layer of complexity. But, you know, the best strategy is open communications. Everyone needs to understand why we're doing this. People at very senior-level positions often have revenue targets written into their performance requirements. Well, if you impact revenue by not being compliant in some of these critical areas, you should lose some of your potential bonus.

While that seems a bit ridiculous, the point is that I worked to transfer accountability from IT Security to the data and system owners, to say, "You're responsible for it. Report back on how you're doing. Here are the tools to use." Then their boss is going to see the level of compliance and determine whether their impact on revenue was positive or negative. Believe me, it caused a lot of stress on executive communications and relationships. But when people are accountable and they understand why something needs to be done and it makes common sense, then they're more apt to do it.

---

*When people are accountable and they understand why something needs to be done and it makes common sense, then they're more apt to do it.*

---

I'm not saying that it always works well. Some people will fight you to the end and not want to be accountable. But having an open-kimono approach to compliance during executive leadership meetings and talking candidly is beneficial. Everyone needs to understand where the organization is deficient across the board and what needs to be done in the future.

**Peter Gouldmann:** As we all know, cybersecurity is a team sport, as you described. The challenge is that everyone has different dragons to slay in their daily job. When you ask



their assistance to help you slay your dragon, their dragon is not getting attention. So, there is a need for prioritization. There has to be some overarching goal established.

All of us come in to do the best job we can and we each face challenges. But usually there are things outside of our control that affect our ability to be successful. We shouldn't hold our colleagues accountable for what we might see as failure, as opposed to the fact that there are things outside of their control. So, at the end of the day, respect for each other, understanding that we're all here to accomplish the same mission and we have different responsibilities, goes a long way to helping build the right kind of environment for team success.

---

*Respect for each other, understanding that we're all here to accomplish the same mission and we have different responsibilities, goes a long way to helping build the right kind of environment for team success.*

---

**Steve Horvath:** If I got in a time machine and went back to 1998 when I started doing information security, my younger self would expect to be told that we were going to fix all this in the next couple years, not that we'd still be dealing with the same problems 20 years later. Seems like sometimes we don't know what's on the network, so it's hard to make sure everything is up to date and patched. We're still facing the same problems with things like a system running Tomcat out on a DMZ that hasn't been patched and thus gets exploited.

The cloud has also brought a tremendous amount of complexity, but also offers an opportunity from a cybersecurity perspective. I'm hopeful that some of these things will be solved in the future. But I still can't believe that we're fighting a lot of those same dragons that we've been fighting for 20 years in our career field.

## **Q: WHAT UNFORESEEN OR UNINTENDED COSTS ARE CAUSED BY AUDIT FATIGUE?**

**Steve Horvath:** There are many costs to consider when we focus on the concept of audit fatigue and its eventual fallout. We can talk about the cost of technology and software, staff, training, recruiting, supply chain, and fines. While some costs, like fines, are largely avoidable if you put a strong and resilient corporate program in place, what are other unforeseen or unintended costs that audit fatigue can cause?



**Lance Dubsky:** No matter where you're working, make sure the tools that you're using – your cybersecurity stack, your audit tools, your vulnerability management – were implemented the right way. I have found that often the expense of buying the tool is expected, but the expertise from the particular vendor was not used to implement it correctly, so it's not necessarily generating the right kind of result. BigFix and LANDesk are just two, but there is a huge list that need to be implemented correctly. If you purchased a tool and think that your internal staff is qualified, sometimes they are, but often they're not. You need to spend the extra money to do the integration with other tools necessary to deliver the right results and the right reporting. Whatever tools you have in your cybersecurity stack, make sure they're doing what you need them to do and that you don't have redundancy unless that was the purpose of the tool. And spend the extra dollars to make sure the tools are implemented the right way to give you the right results.

---

*Spend the extra dollars to make sure the tools are implemented the right way to give you the right results.*

---

**Jean Schaffer:** I agree 100 percent with Lance. You're buying capable tools, but have to actually implement them to do the job that you bought them for to make sure that you're getting the best value from those tools.

Because there seems to be an increasing number of compliance checks and audits with all of the regulations and standards that are coming out, your work force is under increasing pressure. In the past we've worked people so hard at times that they want to take different jobs where they're under less pressure. So you're losing the very talent that you need to keep your cybersecurity organization functioning as well as it can.

One technique to help avoid this is to plot out what audits, what compliance checks you have and the timeframes you have to do them, so you can figure out how to not be under that constant pressure. You may determine to do a security audit once a quarter and then those answers will be the answers, regardless of what compliance check you're actually doing or who's asking the question.

---

*We really need to worry about the workforce and how to address [their workload and stress levels] to ensure we're not running our good talent out the doors.*

---

Employee burnout is a real risk if you don't manage the timing of audits correctly. I feel really bad when we're continuing to pile on more and more of the regulations. I understand why we need new regulations, and I'm in agreement. But on the

execution side, we really need to worry about the workforce and how to address that to ensure we're not running our good talent out the doors.

**Peter Gouldmann:** Thankfully, within the federal government, we're subject to a different kind of cost basis than industry. Most of our associated costs are just the unexpected or unforeseen costs associated with operating the program; usually event driven. We generally suffer from insufficient resources across the board, so the greater challenge is juggling what we have. We see new expense areas as outside of the realm of our resources. There's that constant budget struggle to reconcile.

### Q: WHAT ARE THE PERSONNEL COSTS OF AUDIT FATIGUE?

**Steve Horvath:** A few years ago at Black Hat, people were talking about the depression that many security professionals were dealing with as they tried to beat back the onslaught of threats but were still getting compromised. Not having enough resources to get everything patched or fixed and then the burdens of compliance and audit fatigue.

Telos recently commissioned research associated with audit fatigue across the IT industry, in both the public and private sectors. One of the most unnerving findings was that many compliance professionals had feelings of “personal dread” when facing an audit.<sup>3</sup>



Over four in five (81%) security professionals report that they personally dread when their organization is audited.

Excerpted from *A Wake Up Call: The Harsh Reality of Audit Fatigue*

Considering each of you has been in a position of primary responsibility for the compliance or risk management of a major organization, have you felt significant worry or dread as a result of audits? Has it kept you up at night?

**Peter Gouldmann:** I tend to sleep pretty well. I can push my day job off when it's time to get some rest. But I know that is a bit of an anomaly, because a lot of people are bothered with stress like that.

---

<sup>3</sup> Vanson Bourne for Telos Corporation, *A Wake Up Call: The Harsh Reality of Audit Fatigue*



I worry like everybody else. An audit report is kind of like a promotion list. You want to know what's on it, but you don't want to know that you're not on it. When you see an audit report, you want to see that your team is getting credit for the good work that's being done. And you're hopeful that, in the balance of things where there will always be more that needs to be done, that you're measuring up and that you're doing a decent job.

The dichotomy between operational cybersecurity and programmatic effectiveness that I mentioned at the beginning of this conversation – we haven't figured that out yet. If I had a crystal ball and could solve that, I'd probably be a rich guy. A lot of people are trying to make this work, but we're not quite there. An audit can be helpful in that it points out areas that require attention, but it can sometimes be viewed as unhelpful because it's yet another thing to put on a very long list of things that you have to attend to in the job of maintaining security compliance or even security maturity.

It's an old saying, but it still holds true. We have to be right every time in order to avoid an attack. Our attackers only have to find that one time we're not. It's really hard to know you're working very diligently with your organization's interests in mind to do a good job and support the ability to make revenue or to meet mission requirements, only to have an audit reveal that you have some significant challenges. You might already know it, but now it's visible in print for everybody in the organization to see. That's not always viewed as constructive because you are working hard on a number of areas and they don't always get noted. Sometimes you don't get a sense of accomplishment. So I can certainly see how that could be viewed as dread or stressful.

---

*We have to be right every time in order to avoid an attack. Our attackers only have to find that one time we're not.*

---

**Jean Schaffer:** Like Pete, I'm a sound sleeper. I don't really have that dread coming up for the audits. Intuitively, I always know where our weak points are before the audit finds them. What's important is to make sure that we're holistically looking at cyber, not just with the checklist mentality, and doing the right things to protect ourselves. Then the audit is going to fall where it may.

From my boss's view? Yes. They worry an awful lot because the risks are big. In the Intelligence Community, the risks are really big. Let's do what we know we need to do and do it to the best of our ability. And then, let the chips fall where they may.

**Lance Dubskey:** I would like to echo both Pete and Jean. Back in the late 90s, I was resistant to audits. I was not the most cooperative person, but I found that, especially in a federal environment, if you basically invite the auditor to take a look at absolutely



anything they want to, anything they find is going to uncover the risk of that particular thing or it's going to help you fund your program. You know, if they find some kind of anomaly that you were not aware of.

When I was in government, I trusted my workforce, and I tried to relieve their dread of audits by saying, “It's going to fall on me.” You try to make sure that your teams are shielded from that, although they're not going to be shielded from whatever work comes out of a poor audit result.

On the commercial side, though, there is a lot of dread. Some people are tremendously loyal while others say this is too much work for something that might not be important. Sometimes they do vote with their feet and say, you know, I'm going to seek out a less stressful environment.

That's another reason that you need to make sure that people have the right training, that they have the right support, that they have the right tools to do their jobs, and that you let them know when they're doing well.

---

*Make sure that people have the right training, that they have the right support, that they have the right tools to do their jobs, and let them know when they're doing well.*

---

What do I lose sleep about? I typically would lose sleep over what I don't know. It's easy to know everything that's in front of you. But it's what I can't see that disturbs me. As I have briefed agency directors and deputy directors on the state of security, some would ask, “What are we missing? What is going to bite us? What is the adversary doing that we don't know anything about?” And then they would just leave it open ended. That would cause the most dread because it's a hard question to answer.

## Q: CAN AUTOMATION RELIEVE AUDIT FATIGUE?

**Steve Horvath:** In my opinion, continuing to have a manual approach to risk and compliance activities essentially reinforces a “security checkbox” paradigm that's largely responsible for the audit fatigue issues we are all facing today. With organizations acknowledging serious value in moving some or all of their IT solutions to the cloud, not only for lower costs but also better security, how can they turn to automation to alleviate these issues of audit fatigue?

**Lance Dubskey:** I think every organization should be driving toward automation. Anything you can do to reduce the pressure on people – automation, metrics, reports that tell you something important about the state of security of your organization or the state of privacy of your organization – is very important. Making sure your tool sets work together. You can go best of breed on a whole bunch of tools, but they may not



work well together, or it can be very costly to integrate them. But automation is something that should always be pursued to make life easier for the organization and its people.

**Peter Gouldmann:** I believe we've reached the point in cybersecurity where we have to focus intently on the data and on the people accessing that data. Many of our challenges with visibility are based on our operating networks that are predominantly internal. As we pivot to the cloud, we have less control over the environment, and we're relying on cloud providers to ensure some of that security. So if I'm going to work towards automation, I'm going to work towards the type of automation that allows me to better manage my data and identify its relevance and importance to the organization and apply the necessary handling of controls and oversight. Since data is almost as big, actually bigger, than the number of endpoints we would operate in our network, automation would absolutely help to maintain and monitor data and kick out anomalous activity for human review.

---

*Automation would absolutely help to maintain and monitor data and kick out anomalous activity for human review.*

---

## Q: WHAT WOULD MAKE INTERNAL AUDITS MORE BENEFICIAL?


**Steve Horvath:** Let's get to a question from our audience. How can an internal audit become more helpful than it currently is? What's a good way to structure internal audits that would be more beneficial to the teams that have to deal with auditors?

**Lance Dubskey:** At Iron Mountain, our internal audit team was really fantastic. They stayed on top of all of the different audit findings across the board. At the beginning, I had set this tone with them. Every time an audit question came up, I would say, "That sounds like about a million dollars and about two months' worth of work. So, yes, we can definitely do that when you increase the funding by a million dollars." If you consider that everybody is currently gainfully employed and working hard on everything that they're supposed to be doing for their day job, any additional item they have to validate is going to be an additional cost or require a reprioritization of current ongoing work. So the audit staff became well-schooled on all of the different audits, and we could have discussions and put together matrices related to risk and then schedules of how we might address those. Internal Audit became a partner with IT and Security to figure out the risk level and determine when to address it. And then,

---

*Internal Audit became a partner with technology and security to figure out the risk level and determine when to address it.*

---



because they briefed the board of directors and executive leadership, we were all on the same page regarding what to do. So I always looked at them as a partner.

## Q: HOW DO YOU APPROACH RISK MANAGEMENT OF M&A?

**Lance Dubsky:** Again, at Iron Mountain, we bought a company every month, so over a three-year period, we had bought thirty-six companies. It was a nightmare to integrate those companies and systems into the current infrastructure.

Often, companies are purchased without consideration of what the security impact is. Typically IT and Security only find out after the acquisition has been announced. Then they have to go figure out how to integrate that company's security and compliance programs. You have to find the manpower to put on the ground, to get somebody there to see what the true state is. I know that there are some companies around these days that have really great technology that you can take basically out of the box, plug in, and assess how vulnerable the purchased company is and how challenging it is going to be to integrate.

Most companies are very close hold on the information of the companies that they're going to buy and you don't get it until afterwards. My preferred way would be to have a security engineer on the ground much sooner.

## ADDITIONAL RESOURCES

Many additional resources addressing audit fatigue are available from Telos Corporation. Please follow the links below.

- A [video recording](#) of this conversation during the *Cyber Risk and Data Privacy Summit* hosted by *Compliance Week*
- *A Wake Up Call: The Harsh Reality of Audit Fatigue* – a [report](#) by independent research firm Vanson Bourne, commissioned by Telos.
- An [infographic](#) highlighting the findings of the Vanson Bourne research
- An [on-demand webinar](#) featuring Vanson Bourne Research Consultant Katie Noyce

Telos personnel are always available to discuss the challenges your organization faces in light of the ever increasing compliance burden.

1-800-70-TELOS | [sales@telos.com](mailto:sales@telos.com)  
[www.telos.com](http://www.telos.com)

January 2021  
©Copyright 2021 Telos Corporation. All rights reserved.