VOICES FROM THE COMMUNITY

svb Silicon Valley Bank

SolCyber

SUREFIRECYBER
From Response to Resilience

CONVERGE™

**Grant Bourzikas**
CIO, SVB

**Scott McCrady**
CEO, SolCyber

**Billy Gouveia**
CEO, Surefire Cyber

**Anthony Dagostino**
CEO, Converge

# Cybersecurity Essentials for Funds and Portfolio Companies

## Video description

Grant Bourzikas from SVB, Scott McCrady from SolCyer, Billy Gouveia from Surefire Cyber, and Anthony Dagostino from Converge explain why mitigating cybersecurity risk is now a major responsibility of a fund COO, CFO and CCO.

---

## Video transcription

### Introduction
Starting at 00:09

**Grant Bourzikas:** Hello everyone. My name is Grant Bourzikas and I'm the Chief Information Security Officer at Silicon Valley Bank. I'm responsible for all cybersecurity and physical security across SVB. We have assembled some experts to talk to you about cybersecurity and provide some advice for your private equity and venture capital firms. I'd like to touch on two key risks that I think should be top of mind.

---

### Overall Risks to Manage
Starting at 00:31

**Grant Bourzikas:** The first one is around loss of sensitive data or the theft of data that might be non-public information. The second one, which is really an emerging risk, is the loss of operational resilience. What is the loss of operational resilience? It's where you can't seamlessly deliver your services because of a cyber-attack. From a venture capital and private equity standpoint it is essential that your portfolio is resilient under attack from things like distributed denial service attacks, or ransomware. Things that can help are education of your employees, understanding critical vendors, third party, fourth party, fifth party, and understanding what critical controls, you need to apply, or how attackers could compromise your organization. Now I'm super excited to turn it over to Scott who will discuss how you can improve your security posture.

## Improving Your Security Posture

Starting at 01:27

**Scott McCrady:** Hi, I'm Scott McCrady. I'm the CEO of SolCyber and we help financial services organizations and mid-size companies increase their security posture. I tend to get asked two questions on a very regular basis. And so, the one I get asked the first and most often is, “is the threat real or is it just hype?” The main thing I'd say to that is unfortunately it's very, very real. And we really try hard in our organization not to spread fear and doom and gloom, but the reality in the stats is pretty bleak. Currently we're looking at about a one in three chance of organizations being breached on an annual basis. So that's just not good. You can see that reflected in some financial statistics. The first one being that 50% increases in cyber insurance are very common right now. And also, we're seeing about one in three rejection rate for your cyber insurance policies.

So, all the way around, there's just a significant amount of risks that's come into the market that's reflected and makes it very difficult and challenging obviously for CFOs to manage that. And we're here to try to help with that. The second piece and the second question I get asked is, "This has always traditionally been an IT problem. Is it still an IT problem?" And I think that's a well framed question because it's true, but it's really shifted to more of a business risk problem.

And so, one of the things we'll talk about here today is the fact that you really want to top and tail your overall security posture and your security organization, with the ability to have incident response and instant response retainer, to help with something that happens. You want cyber insurance to mitigate that business risk, and you really want to increase your security posture all the way around. So hopefully you don't have to utilize either of those two policies.

So, what we're really trying to do here from our side is to give you guys some good information around how the business risk has changed. And hopefully that's useful for you. With that I'll transition to Billy, who's going to talk a little bit about incident response and incident response retainers.

---

## Improving Your Incident Response

Starting at 03:27

**Billy Gouveia:** Thanks very much, Scott. That's great. My name is Billy Gouveia, and I lead a cyber response firm named Surefire. Let's begin by providing some comments about how and why companies can prepare for cyber security incidents. Organizations that haven't prepared for cyber incident can expect long business interruption times, high legal and regulatory risks and chaotic and costly responses. Here are three things that I can offer CFOs and other business leaders to provide some reassurance.

First, have a plan. Second, exercise that plan and third get cyber insurance. Let me step through those three things in turn. Regarding having a plan, this isn't the time for a pickup game, determine who you're going to work with and build relationships so you can bring the right experts together and respond decisively. No matter how capable your technology team is, business leaders should seek expert advice on decisions, such as whether to make ransom payments, determining how to notify regulators and customers, how to take advantage of the crisis to strengthen your cybersecurity posture. Negotiating ransom amounts, for example, is not the type of thing that you want to do without experienced help.

Second, exercise a plan. Exercises build confidence, confidence that you have the right experts on your team, confidence that your critical data is properly protected. And most importantly confidence that your company's leaders can come together, assess the situation realistically and keep your organization moving. Third, cyber insurance is not only a risk transfer mechanism, but also a vehicle to help you gain access to the experts who will help you. Cyber insurance carriers will appoint a specialized law firm known as a breach coach. A breach coach will designate an insurance response company to serve as a quarterback. Without having cyber insurance in place, may take many days to get agreements in place with these experts and get their assistance. Anthony, an expert in cyber risk management is now going to talk more about the importance of cyber insurance.

---

## Mitigating Business Risk with Cyber Insurance

Starting at 05:22

**Anthony Dagostino:** Thanks, Billy. Great insights. Hello everybody, I'm Anthony Dagostino, CEO and Founder of Converge. The next generation cyber insurance provider. Now Billy talked about the benefits of having insurance and the balance sheet protection and how it can really be critical in the time of response, which is true. And why is insurance so important? And it's just like any other line of insurance, we buy it to protect against the claims, but from a balance sheet protection aspect, but also reputational aspect.

And there was a claim study last year that was done that shows the magnitude of what these ransomware losses are taking on companies. And it doesn't matter if you're at the firm and fund level for private equity or venture firm, or a portfolio company of one, the impact is still sizeable. And we found that the average ransomware payment is close to $1.5 million. That's after being negotiated down. What's even more staggering is the business income loss. That's that ensuing loss of the net income impact, if you don't have the right backups in place, and that was close to $5 million in this recent study.

When you add all the costs together, it's close to $7 million on an average ransomware claim. That's the money paid by insurance companies. Now, while that's staggering, we buy insurance in case that does happen and to protect the balance sheet. But what's been really good about the insurance industry lately, is all these ransomware attacks that are happening have caused the cyber insurance providers to look at what went wrong. What was the root cause? And what you see is there's about nine critical controls that companies need to have in place to not just protect themselves from ransomware attacks in the first place, but to also get the best and broadest insurance coverage.

And that includes things like multifactor authentication, backups that are offline and regularly updated. Having managed detection and response systems in place deployed across all endpoints and having a really good incident response plan test. So, whether you're at the firm or fund level and looking out for the information that you're holding on limited partners and portfolio companies, or you're a portfolio company yourself, and you're thinking about the data that you have and what would happen if you were brought down in the income that you will loss, insurance is an important piece of that puzzle. So, with that, I'm going to hand it over to Scott. Scott, over to you.

---

## Conclusion

Starting at 07:39

**Scott McCrady:** Thanks Billy. Thanks Anthony. Now to conclude the video, I want to leave you with one final thought, which is how do you transition your organization to protect it against today's modern threats? And to keep it super simple, traditional security has really been a perimeter base game. We used to call the crunch exterior with the soft gooey middle and transitioning to what we call a modern security posture, which is very user based, so that your users are protected regardless of whether they're working from home, the office on the road or anywhere else. And if you do that, you put yourself into a position to understand the risks, to see if you're a target for cyber activity and to be able to respond accordingly. So, with that, I'm Scott McCrady, thank you very much for your time.