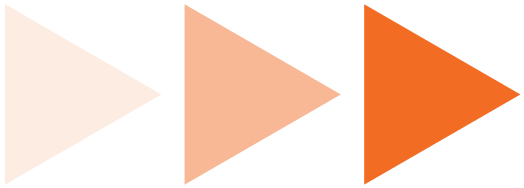
a guide to talking about security risk.



CompTIA | IT Security COMMUNITY

Are you doing enough to protect against IT Security threats?

READ MORE ▶

Right now is the best time to talk about a risk assessment.

Businesses think they're in control of this difficult, but vital process. It's easy to forget how dynamic the danger really is. Cyber criminals rely on complacency and it's up to security experts to elevate the conversation.

Regular assessments are crucial.

Information security risk assessment needs to be an ongoing process of discovering, correcting and preventing security problems. A risk assessment is part of the NIST framework and is composed of six methodical steps.

NIST's 6 Steps to a Risk Assessment:

1. Identify the Systems
2. Identify and Document Internal and External Threats
3. Determine Risk & Impact
4. Analyze Controls
5. Determine the Likelihood of the Risk
6. Identify and Prioritize Risk Response

common objections

Businesses can underestimate the need and frequency of assessments. We'll explore the following frequent objections and rebuttals:

- I'm too small
- My data isn't valuable
- We're handling it
- It's too expensive
- It takes too long
- We already had one

the objection

1. I don't need a security risk assessment. I'm too small.

the response

Cyber criminals are on the lookout for small businesses who think like that.

the conversation points

- They're on the hunt for an open door and small businesses, especially ones who think like this, are an easy target
- Cyber security resources and expertise are scarce in small business, so they have the most vulnerabilities

the objection

2. But my data isn't valuable.

the response

Really? Because client and employee data is extremely valuable on the black market.

Personal data can be sold in the US for $233 per record, with healthcare data going up to $408.*

* Source: Ponemon Institute

the conversation points

- Only 14% of small businesses are completely satisfied with their current security posture
- Now is the time to take a more proactive approach for your business
- Small steps towards a strong security posture can make the difference between a small business thriving or struggling

the objection

3. We've got it covered.

the response

Things change all the time and what if you missed something?

the conversation points

- Would an employee tell you if they found something that might get them fired?
- Is your business up-to-speed on the latest security protocols?
- Checks and balances are a best practice across the board. That's why a CPA checks your books at tax time

the objection

4. It costs too much.

the conversation points

- The global average cost of a breach is $148 per lost or stolen record*
- Two-thirds of small businesses go under within six months of a breach
- A risk assessment will give insight about where to efficiently spend your IT budget dollars and how to build a strategic plan

the response

Can you afford not to?

As technology continues to evolve, security must evolve with it. A decade ago IT departments weren't talking about cloud services, BYOD, etc. but as technology continued its exponential growth, those things became table stakes. Good security practices are a competitive advantage.

* Source: Ponemon Institute

the objection

5. It's too time consuming.

the response

Security risks change all the time and it's crucial to stay on top of them.

the conversation points

- Isn't the time worth protecting your brand and your most valuable data?
- What about the customers who entrust you to do everything you can to guard their information?
- Isn't preventing a problem far less time-intensive than fixing one?

Partnering with a solution provider to examine your current risk is time and money invested in your future. It is part of the foundation of your business' stability and ability to grow. The truth about security incidents is that it's not IF a company will have one, but WHEN.

the objection

6. We already had a risk assessment.

the response

Cyber criminals are always exploiting new opportunities. They rely on your complacency.

the conversation points

- Your information and IT environment change daily
- Your previous assessment was a “snapshot in time”
- Security risks change frequently (new threats emerge all the time)

Security assessments should be a lifecycle, done periodically. Additionally, most traditional security is reactive. Periodic assessments help you become proactive. As the volume of attacks is rising, companies need to give serious thought to the way they are securing assets and protecting customer and employee data.

Let's keep the conversation going.

Staying on top of risk means continually assessing threats. Don't give cyber criminals an opportunity to get at your valuable data or wreak havoc on your systems.

Take the first step with the **IT Security Assessment Wizard**

START NOW ▶

Arm yourself with more resources at **CompTIA.org**

LEARN MORE ▶