CYBERSECURITY

Where you spend is more important than how much you spend

ClearTone Consulting, LLC
Technology Strategy Leadership

Cybersecurity

Where you spend is more important than how much you spend

Brian Scott, President, ClearTone Consulting LLC

On a weekly basis, there is a steady stream of news regarding cybercrime attacks. In fact, with the spread of the COVID-19 pandemic , the US FBI has reported a 300% increase in cybercrime activity. The data tracking the number of ongoing cyber attacks and the costs associated with compromises continues to increase at an exponential rate. This growth continues despite the fact that most organizations continually increase their cybersecurity investments.

Change occurs so quickly in the world of cybersecurity risk that many protection systems will check for new risk signatures every few minutes. A primary contributing factor to the rate of change in risk is that cyber criminals are utilizing the same innovations in technology available to the public, but leveraging them to create new and automated threats. Most cyber attacks are automated and executed by a countless number of bots or robotic applications designed to execute millions of attacks every second. They are also utilizing advances in artificial intelligence to improve their ability to find vulnerabilities.

Following are some common misunderstandings regarding cybercrime. Organizations that are operating under some of this misunderstandings are likely not protected as well as they could be and are not maximizing their investment in security.

1 Myth 1 - All assets must be protected the same way

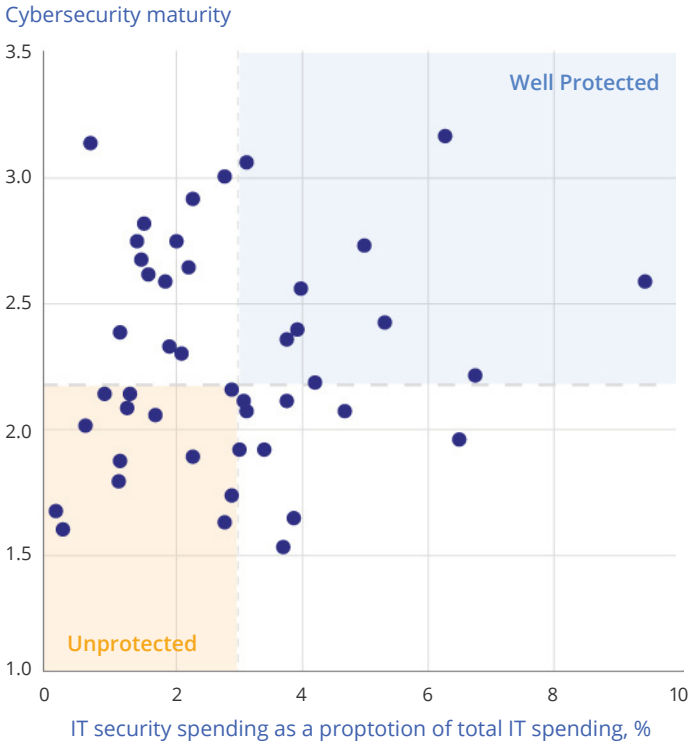
Some IT organizations approach their protection strategy with a one-size-fits all perspective. Think of your organization as a house with many rooms - each with its own set of doors and windows. It is expensive to deploy top-of-the-line protections at every single window and door throughout the entire house. In reality, all of the rooms do not contain the same level of digital assets with some being far more valuable than others. It may be more cost effective to segment your organization's assets and protect them with levels appropriate to their value for the business. Put your most valuable possessions into a safe.

2 Myth 2 - The more we spend, the more we are protected

If there is one golden rule in cybersecurity, it is that where you spend your money is far more important than how much you spend. Make no mistake, cybersecurity is and will continue to be an area requiring increasing investments in years to come, but the pace of growth can be tempered by intelligent, focused decision making.

As can be seen in the following diagram comparing company spending to cybersecurity maturity, it's clear that spending alone does not equate to protection. Areas of the chart to note are that there are many companies surveyed that have significantly more spending and yet have not achieved any greater maturity than others with less spending. Additionally, there are several companies that have a relatively low spend but have achieved the same level of maturity as companies with significantly more spend. This data indicates that it is the cybersecurity strategy itself that determines the outcome of protection and not the spend alone.

Companies' spending on cybersecurity does not necessarily correlate with level of protection



This data reflects responses from 45 companies in the Global 500 about their cybersecurity spending and capabilities. Companies' cybersecurity maturity is rated on a scale of 1 to 4, with 4 being the most mature (highest-level talent and capabilites). Spending is rated on a scale of 1 to 10; no companies allocated more than 10% of their budget on security.

Source: 2016 McKinsey Cyber Risk Maturity Survey

3 Myth 3 - Hackers are only a threat to large corporations

43% of all cyber attacks are aimed at small and medium businesses. Because so many attacks are automated, the size of the organization is inconsequential. This is particularly true for ransomware attacks. If fact, smaller organizations are usually the better target for ransomware as they often have underdeveloped protections.

The State Of Ransomware Among SMBs

In the last 12 months

22% of organizations had to cease business operations immediately because of ransomware

65% have suffered a data breach

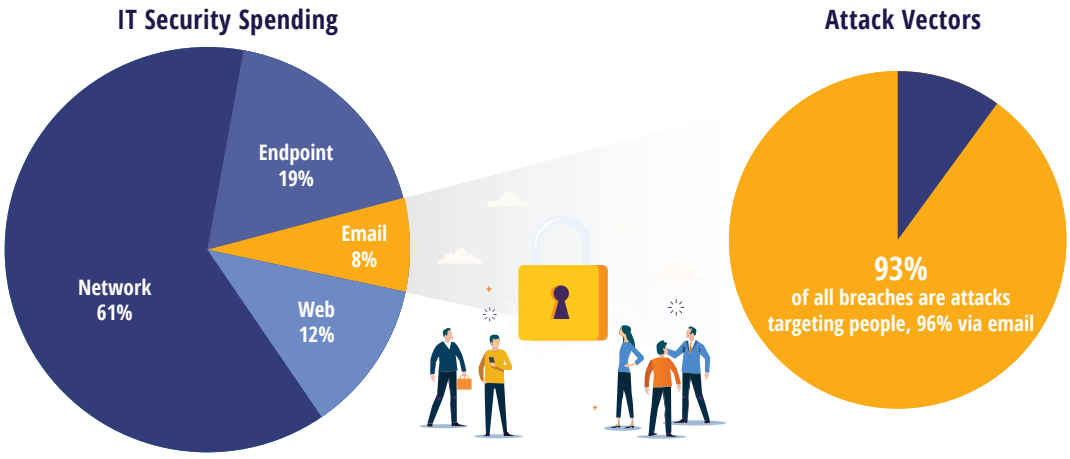
81% of businesses have experienced a cyberattack

35% were victims of ransomware

4 Myth 4 - Unprotected systems connected to the Internet are your biggest risk

Did you realize that your biggest assets are also your biggest cyber risks? The same committed individuals that work hard every single day to satisfy customers and grow your revenues are the ones that will unwittingly expose information that leads to a compromise or download malicious software that attacks your systems. An effective training program must be at the forefront of your cybersecurity program.

Defenders Don't Focus on People, but Attackers Do

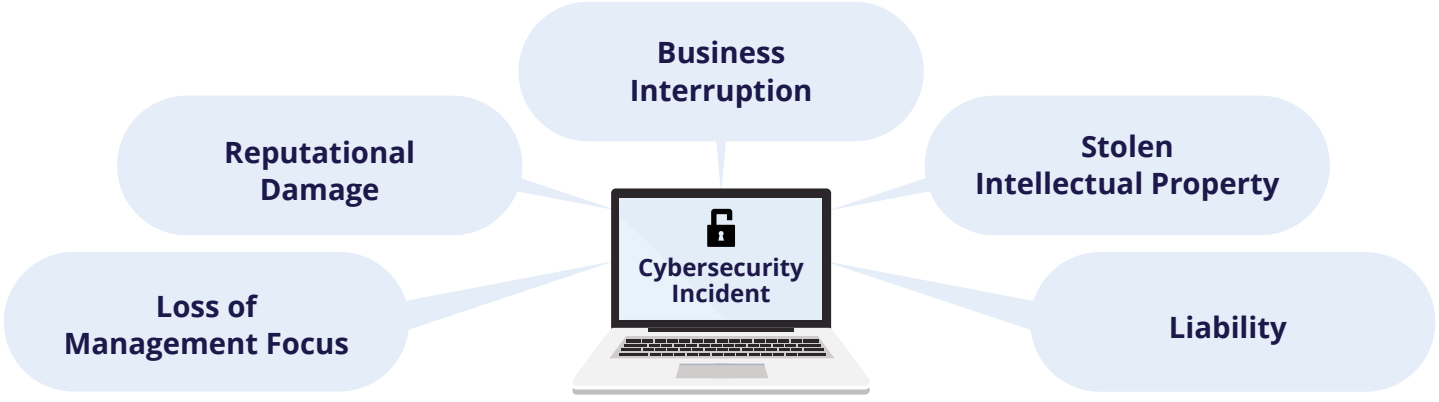


Source: Gartner Information Security, Worldwide 2016-2022, 1Q 2018 update (2018 forecast)

Source: 2018 Version DBIR

5 Myth 5 - Cybersecurity is a technology problem

Cybersecurity is a business problem, not a technology problem. The support of this claim lies in the previous myths. To effectively protect your organization, it takes buy-in and commitment from the president, the leadership team, and the entire organization. This can only be achieved when the problem is viewed for what it is – a business challenge.



In Summary

Leveraging the experience of a seasoned technology executive can help the leadership of organizations of all sizes understand their current cybersecurity risk position, envision the appropriate security position with a balanced, cost-risk perspective, and create a security roadmap to ensure the critical initiatives are accomplished in an appropriate timeframe.

ClearTone Consulting, LLC
Technology Strategy Leadership