Security breaches are the most intimidating threats for CISOs and security executives. Because of that, upper level management, shareholders and even consumers are focusing now more than ever on the security department. With that, CISOs need to see this as an opportunity to work closely with business stakeholders to incorporate cybersecurity strategy with their organization's business initiatives. This is an ideal opportunity to address skill shortages and increase professional development of the internal security workforce.

Takeaways:
1. How the CISO’s role has changed
2. The latest security threats and how they can positively impact your team
3. How to measure your team’s shortcomings and areas for improvement

We will explore key learnings from various industries and verticals on the good, the bad and the ugly of digital transformation. We will have an opportunity to not only be exposed to successful use cases, but also ask the hard questions behind those successes.

Takeaways:
1. One of the best ways to learn is to hear the stories of success (and failure) from companies similar to yours.
2. Asking questions of HOW the journey unfolded are just as important as the end result
### Takeaways:
1. Understand the latest regulations, such as GDPR
2. How to tell your CEO and other business stakeholders that data protection can be a key differentiator for your organization
3. The steps needed to take to be regulatory compliant

### Networking Break

### Thought Leadership

**Closing the Gap of Grief: Business Driven Security**

How bad is it? When a breach occurs, how confident are you that you can quantify the impact to the organization in language they understand? This session describes the requirements for closing the gap: Complete visibility, to paint an accurate picture of what's happening across the environment. Faster insight, through better analytics and detection capabilities. Business context around incidents. And finally, more effective response, where security teams are certain they are taking the right actions to reduce risk and are sure they are protecting what matters most.

Takeaways:
1. Learn how to garner the right visibility, in the right context to defend what matters most
2. Discover the 6 steps to take command of your evolving security posture in this uncertain, high risk world
3. Find out what it takes to link your security strategy with your business priorities

### Executive Exchange

**Executive Exchange**

### Think Tank

**The Solution for Your Legacy System's Security: The Cloud**

Over lifespan of an organization, CIOs/CISOs have developed and implemented technologies that has been key to the organization's success. However, CISOs and their security teams today find themselves stuck ensuring that legacy systems are secure. The solution is cloud-delivered security products that are more agile with the ability to implement new detection methods and services faster than on-site solutions. While cloud security is an ideal solution, it is important to know that using the cloud is more than moving legacy management servers to the cloud.

Takeaways:
1. Review the status of legacy system security
2. What cloud solutions are the best fit for their business
3. What are the main needs in regards to system's scale, data telemetry, staff growth, machine learning, API-based access, and more

### Solutions Spotlight

Deep dives into the latest and greatest technology solutions to today's business problems.

### Executive Visions Panel

**The Revitalizing Change in the Role of the CISO**

A CISO’s role, goals and objectives have drastically changed over the years as most CISOs supervise teams and units beyond their IT’s security. Because of these changes in responsibilities, a CISO’s success is measured in greater business metrics. As a result, the role of a CISO has become both more attractive and more demanding.

Takeaways:
1. What are the significant changes regarding the role of the CISO
2. How to keep up with the changing requirements
3. How to properly measure a CISO's success

### Closing Remarks

**Summit Networking Happy Hour**

**Welcome Dinner & Entertainment**

**After Dinner Networking Reception**

---

**Wednesday, November 18, 2020 - CISO Midmarket Summit**
AI: a CISO’s Best Friend

It does not take an expert to know that information security threats will only continue to increase. That said, AI is proving to be a worthy defense against these threats. Leading enterprise organizations are investing and relying on AI-based security systems and analytics. As this trend continues, AI-defense will only continue to grow and improve.

Takeaways:
1. The future of AI-based security and how it will impact your organization
2. The latest threats and how AI-based security can help
3. Create awareness for your stakeholders to gain support behind AI-based security systems

Keynote Presentation
Addressing Privacy on a Global Scale

Of all the risk management issues that present themselves to the modern-day CISO, perhaps the most difficult to address is that of privacy. In and of itself, privacy is no different a challenge than protecting any other sensitive information, however the multi-jurisdictional impacts of the issue due to wildly differing laws between the US and European countries make this an issue that is often times overwhelming to address. CISOs must work diligently to ensure that their privacy efforts conform with the standards of any jurisdiction with which they might work, where their data might be held and this is an almost overwhelming task.

Takeaways:
1. Privacy is one of the most challenging issues for any business and CISO to address
2. The difference in regulations between and among European countries (both those in and out of the EU itself) and North American ones means traversing a fraught landscape
3. A strong approach to privacy that addresses global differences is essential to being a stable and viable global business

Think Tank
Machine Learning Is Here to Help, Not Replace

Over the next few years, machine learning (ML) will be a regular security practice and will offset skills and staffing shortfalls. Today though, ML is better at addressing smaller, more specific problems. Technology leaders have to understand that humans and machines complement each other and work better together than alone, as ML can assist humans in addressing uncertainty by presenting relevant information.

Takeaways:
1. Discuss the ways machine learning can assist teams and organizations
2. How to make the right machine learning choices for your organization
3. The future of machine learning

Thought Leadership
Machines Are Friends Not Foes: Cognitive Computing Accelerates the Journey

Popular movies, books and television shows typically position advanced technology as a threat to humanity and all we hold dear. Yet cognitive computing technologies such as Artificial Intelligence (AI), Machine Learning (ML), Natural Language Processing and Augmented Reality (AR) are helping CIOs and CISOs make better decisions faster.

Takeaways:
1. We will discuss how cognitive computing can help us navigate the acceleration of activity and decisions that we are experiencing on our digital transformation journeys.
2. New cognitive computing technologies can be unnerving and difficult to trust.
3. Used properly, cognitive computing technologies such as AI, ML and AR can provide data to humans in such a way to enable us to better prioritize the decisions we must make and make those decisions more effectively.

Networking Break

Thought Leadership
How to Prevent a Costly Attack

Cybercrime has impacted virtually everything and everyone, at some level. Whether it’s a big bank or hospital, a hotel chain or transit system, cyber-attacks affect organizations and individuals alike. Industry experts and analysts agree: cybercrime rates will continue to increase in 2018. In this session we’ll discuss common attack types and threat vectors and how your firm can approach cybersecurity to prepare for inevitable attacks.

Think Tank
Geopolitical Landscape’s Effects on Organizations

The recent U.S. government bans against Russian-based security products and Chinese smartphones are the latest results of suspicion and distrust of competing world powers. Organizations working with government entities must be aware of the geopolitical stipulations regarding their business relationships. Even with the geopolitical landscape, the buying decisions of security products are still based on trust in the supplier. It is important for CISOs and security leaders to incorporate geopolitical risk in all business-critical software, hardware and services purchasing decisions - even if that means considering local alternatives.

Takeaways:
1. Review the geopolitical landscape and how it has effected industries and organizations
2. What to be aware of with your buying decisions
3. What to anticipate and prepare for in the coming years

Executive Boardroom
Driving Digital Transformation: Proactive Path vs. Reactive Response

Shakespeare wrote that we should be afraid of greatness as “some are born great, some achieve greatness and some have greatness thrust upon them”. This is true today as well for CIOs and CISOs. Digital transformation will happen, the only question being will the CIO drive it or will it be thrust upon them. We will discuss how to be a proactive voice in driving your company’s digital transformation journey instead of waiting and responding to the voice of others.

Takeaways:
1. Digital transformation is happening with or without our actions. The most successful CISOs will drive this transformation from a proactive point of view instead of reacting to internal and external voices.

The Importance of Engaging CISOs in Digital Transformation

The digital transformation challenge is significant for all, but CIOs need to understand the importance of engaging their CISO as well. Capturing IoT data from capital assets is a challenge on its own; however, many also struggle with the workforce's preference for entrenched processes as well as the executive team's expertise for managing physical assets, which is contrasted by their discomfort with digital transformation.

CISO: The “Cultural” Information Security Officer

It is well-known that CISOs "wear many hats" and are responsible for more than ever before. One of those major responsibilities is driving a culture of innovation and organizational success throughout not only their team, but the entire organization.

Takeaways:
1. The steps towards establishing a positive and productive culture
2. The major threats to CISOs and their cultural innovation
3. Shared success stories from CISOs who have implemented a cultural change

Navigating Security & Risk in a Changing IT Landscape

Agile, DevOps, containers, microservices and the cloud are all seeing increased adoption across the enterprise. But, while there are valid business reasons to embrace these new models, there is potential risk in implementation. Is this change necessary? If so, how can this change be accommodated effectively, safely? This session will cover some common elements of the risk of change - and of not changing - and suggest approaches to minimize risk as you adopt these new technologies.

Takeaways:
1. The IT Landscape will continue to change leading to new processes, new technologies and new "standard" ways of doing IT business
2. This changing Landscape will present security challenges where you will need to balance the "pain of same" vs the "pain of change

Think Tank

Becoming More Decentralized

Today, increased centralization has put the power and trust into the hands of the few big players. This, of course, raises many security concerns. The risk of disruptions and undesirable outcomes increases as centralization opens the door to exclusive possession or control of commodities and services. As a result, technologies like Blockchain have been implemented to create decentralized alternatives as they move computing resources away from centralized servers.

Takeaways:
1. Evaluating the risks of centralization on availability, confidentiality and resiliency
2. Exploring decentralized technologies like Blockchain and edge computing that offer visibility as well as enhanced security for your organization.
3. Understand the fact or fictionalization of developing AI strategies and the cause for concern for decentralized AI models

Where is the Top Talent?

One of the major challenges for CISOs is finding top information security talent. However, look at 2019 as an opportunity to begin your search with universities and colleges that are expanding their cybersecurity programs due to the shortage of cybersecurity professionals. This session will also cover how to recruit and hire top cybersecurity talent.

Takeaways:
1. Where to seek out the best cybersecurity talent
2. The red flags to watch out for with incoming applicants
3. The importance of focusing on retention

What's the Next Stop On the Transformation Journey?

Our Governing Board will summarize the learnings from the day and discuss the path forward for building an ongoing community of CISOs, where common issues can be addressed and success stories can be shared.
Takeaways:

1. Building an ongoing community with your peers can be an invaluable resource for tackling the digital transformation projects ahead of you.
2. Sharing stories of success (and failures) is not reserved to a one-day CISO Summit, but should be shared on a regular basis with your peers.

<table>
<thead>
<tr>
<th>5:20 pm - 5:30 pm</th>
<th>Closing Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>5:30 pm - 7:00 pm</td>
<td>Summit Happy Hour</td>
</tr>
<tr>
<td>7:00 pm - 8:30 pm</td>
<td>Networking Dinner in the Winery</td>
</tr>
<tr>
<td>8:30 pm - 10:00 pm</td>
<td>After Dinner Networking &amp; Entertainment</td>
</tr>
</tbody>
</table>

Thursday, November 19, 2020 - CISO Midmarket Summit

| 8:00 am - 12:00 pm | Golf Tournament & Spa Appointments |

Optional - Sign-up and Pricing available upon request