PROFESSIONAL DEVELOPMENT ACADEMY

FOR ENTERPRISE CYBERSECURITY

# THE BIGGEST CHALLENGE IS CYBERSECURITY READINESS

# THE BIGGEST CHALLENGE

Leadership development is the most pressing issue of our day. The success of any organization depends on high-performing teams with strong leadership. Nowhere is this more important than among information security professionals.

Every information security officer and risk manager desires to do more for their teams when it comes to leadership development. They want their analysts and other security personnel to become not only trusted business partners, but importantly, to become leaders for the business. The sheer number of professionals in need of personal mentoring from executives with practical and relevant experience makes it nearly impossible to keep up with the demand for more leaders and leadership capabilities. Until now.

At the request of the CISO community, Evanta has collaborated with industry thought leaders, prestigious academicians and security officers to design the professional development academy for enterprise cybersecurity readiness. The focus is on leadership. The result is a 12-week, intentionally designed and wholly integrated social learning journey that transfers insights and knowledge from experienced executives to those at the front line who need it the most.

THIS DOCUMENT DETAILS THE PROFESSIONAL DEVELOPMENT ACADEMY FOR ENTERPRISE CYBERSECURITY.

## MEET YOUR FACULTY

General Colin Powell, CISO Coalition National Leadership Board Members, Fortune 1000 CISOs, distinguished faculty members from prominent universities (including Northwestern and University of Michigan), and thought leaders, including Marshall Goldsmith, provided knowledge and insight to design and develop the Professional Development Academy for Enterprise Cybersecurity. The following is a list of faculty members.

- Dr. Edward G. Amoroso, SVP & CSO, AT&T
- Ramón Baez, SVP & Global CIO, Hewlett-Packard Company
- Joshua Beeman, University Information Security Officer, University of Pennsylvania
- Jeff Brown, Security Architect, Celanese Corporation
- John Bruggemann, CISO, GE Energy Management
- Michael Pozmantier, Program Manager, Transition to Practice, Cyber Security Division, U.S. Department of Homeland Security
- Tim Callahan, VP & CISO, Aflac
- Anthony Caruso, CyberSecurity Advisor, Apache Corporation
- Gerhard Cerny, VP & CISO, AmerisourceBergen
- Darren Challey, VP, Enterprise Information Security, Expedia
- Dan Chisum, Mgr., IT Security & Policies, ConocoPhillips
- Roland Cloutier, Global CSO, ADP
- Jim Connelly, VP, CISO, Lockheed Martin
- Mark Connelly, CISO, Thomson Reuters
- Mike Coogan, Director, Info. Security, Waste Management
- Dale Danilewitz, EVP & CIO, AmerisourceBergen
- Jody Davids, CIO, Agrium
- Christopher Bullock, CISO, Aaron's, Inc.
- Robert L. Dethlefs, Founder & CEO, Evanta
- Deborah Dixson, SVP, CISO, Best Buy Co., Inc.
- Louie Ehrlich, Former CIO, Chevron Corporation and President, Chevron IT Company
- Alonzo Ellis, Sr. Manager, IT Security, Vanguard
- Brian Engle, Executive Director, Retail Cyber Intelligence Sharing Center
- Dave Estlick, Information Security Chief, Starbucks Coffee Company
- Ashley Ferguson, Manager, IT Risk Mgmt., Energen
- Martin Fisher, Manager IT Security, Northside Hospital, Inc.
- Lynda Fleury, VP & CISO, Unum Group
- Michael Frederick, Manager of Support Services, Hormel Foods Corporation

Faculty Continued >

## > Faculty Continued

- Marshall Goldsmith, Author and World Renowned Business and Leadership Thinker
- Tariq Habib, CISO, Metropolitan Transportation Authority
- Christopher Hall, CISO, BNY Mellon
- Ryan Halley, Director, Professional Development Academy
- Malcolm Harkins, Executive Vice Chair, Professional Development Academy
- Stephen Hendrie, Director of Information Security, The Hershey Company
- Robbie Hudec, Global IT Security Director, Novelis Inc.
- Paul Hershberger, Director IT, Security Risk & Compliance, The Mosaic Company
- Patrick Joyce, VP, Global IT & CISO, Medtronic plc
- Wes Hargrove, SVP Development, 7-Eleven
- Harry M. Kraemer, Former Chairman & CEO, Baxter International, Kellogg Graduate School of Management, Author, "From Values to Action"
- Jay Leek, CISO, Blackstone
- John Marcante, CIO and Managing Director, Vanguard
- Jon McNaughton, Professor, University of Michigan
- Joanne Martin, CISO-IN-RESIDENCE, Vicinage
- Thornton May, Leading IT Futurist
- Robert Mims, CISO, AGL Resources
- Keith Morales, CISO, Federal Reserve Bank of Philadelphia
- Tom Murphy, VP, IT & University CIO, University of Pennsylvania
- Randy Nitowski, IT Director, Infrastructure, Subaru of America, Inc.
- Jim O'Conner, CISO, Cargill
- General Colin Powell, United States Army (retired), Author, Diplomat
- Douglas DeGrote, CISO, Director of IT Security & Risk Management, Xcel Energy Inc.
- Tim Rahschulte, Chief Learning Officer, Evanta
- Mark Reardon, CISO, Georgia Technology Authority, State of Georgia
- Derek Rude, Director, IT Security, Weatherford International
- Michael Santarcangelo, Catalyst, Writer, & Speaker, Security Catalyst
- Pete Selleck, Chairman & President, Michelin North America, Inc.
- Curtis Simpson, Director, Enterprise Sec. & Support, Sysco Corporation
- Suzie Smibert, Director and Chief Information Security Officer, Finning International, Inc.
- Cheryl Smith, CIO Emeritus, McKesson Corporation
- Dave Snyder, Chief Information Security Leader, Independence Blue Cross
- Greg Sutherland, CISO, McKee Foods
- Mike Towers, VP, Information Security Officer, Actavis plc
- Marc Varner, CISO, McDonald's Corporation
- Mark Viola, VP, Global CISO, Henry Schein, Inc.
- Michael Wilson, VP & CISO, McKesson Corporation
- Steven Young, VP, Security & Risk Management, CISO, Kellogg's

# PROGRAM OVERVIEW

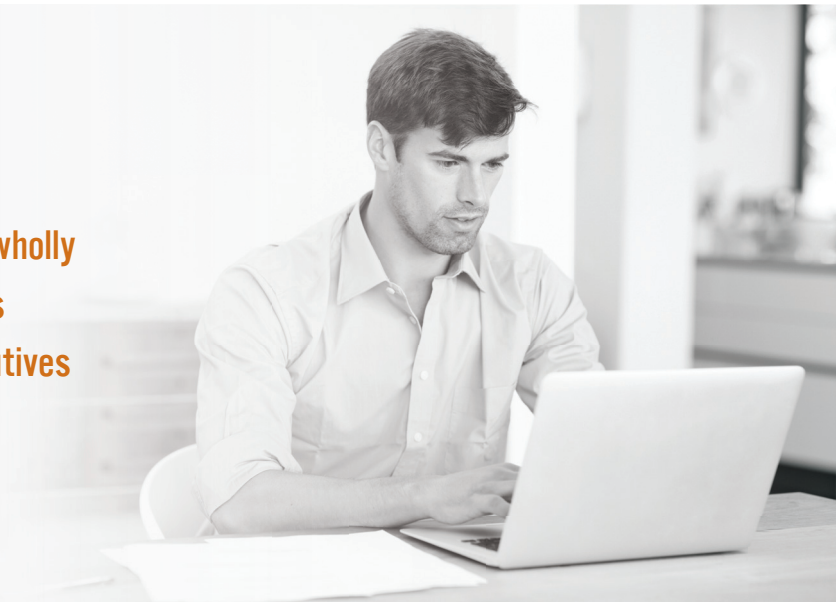
Information security is no longer a peripheral focus for corporate America; in the wake of massive breaches to Fortune 500 companies with costs in the billions of dollars, cybersecurity has become an essential element of protection for enterprise organizations, universities, public utility companies and government agencies alike.

Everyone is at risk. With unceasing attacks from sources around the globe, the question is not if you will be breached, but when and at what cost.

Security readiness is imperative, and the only way to be continuously ready is through continual and collaborative learning – social learning among peers and colleagues in an environment that fosters knowledge sharing while maintaining privacy and security.

For more than 10 years, Evanta has been facilitating leadership development among industry-leading executives from the nation's largest companies. Evanta uses the "by CXOs, for CXOs" model to build regional leadership events that foster collaboration in a safe, nontoxic environment where leaders can come together to access their greatest assets: their peers. Now, those individual who have benefited from Evanta's events are working together to prepare the next generation of leaders by sharing their wealth of experience and knowledge. This is the foundation of the Professional Development Academy – a program designed by CXOs for the next generation of leaders.

**The Professional Development Academy for Cybersecurity is an intentionally designed and wholly integrated social learning journey that transfers insights and knowledge from experienced executives to those at the front line who need it the most.**



## THE CORE TENETS OF THE ACADEMY

Before developing the program, thousands of CISO, CIO, CHRO and other executive voices were heard, along with insight from thought leaders, executive coaches, researchers, and academicians.

| | | |
|---|---|---|
| 1 | ACCESSIBLE | The custom-built online platform enables all course content to be consumable anytime, anywhere. Importantly, the program is affordable and scalable for one member of a team or the entire cybersecurity team. |
| 2 | RELEVANT | Content is timely and relevant, and provided by CISOs, executives and educators. And, the program is expertly moderated in a way that engages both the participant and his or her supervising manager. |
| 3 | EFFICIENT | The program consists of 12 one-week models, each designed in (bite-sized) learning bursts of activities that take 30–60 minutes per day to complete. This maximizes the ROI and is nondisruptive to busy schedules. |

All of the data gathering (from focus groups, one-on-one conversations and industry research) uncovered the need for the program to be built on three core tenants: **ACCESSIBILITY**, **RELEVANCE** and **EFFICIENCY**.

With accessibility, relevance and efficiency as the core tenants of the program, research also unveiled the capabilities gaps. Five capabilities emerged from dozens of others. All of them are the "soft skills" of leadership. We heard time and again that the technical skills are good, but the soft skills are woefully lacking. The following table illustrates the needed competencies and associated rationale for each.

| KNOWLEDGE AND ABILITIES GAP | COMPETENCY | CISO EXPECTATIONS |
|---|---|---|
| LEADING AND MAKING DECISIONS | LEADING | Execute as a (business) leader to facilitate, influence, persuade and negotiate with individuals, teams and groups toward decisions |
| PLANNING AND MANAGING CHANGE | ADAPTING | Leverage the power of systems thinking to mitigate risk and empower people during organizational and market fluctuation |
| BUILDING STRONG RELATIONSHIPS | COLLABORATING | Establish alignment of individual purpose with team meaning and company mission to energize efforts and maximize results |
| PRESENTING INFORMATION CLEARLY | COMMUNICATING | Manage messaging based on stakeholder need, sensemaking and simplicity to create clarity in meaning, confidence and community |
| EXECUTING TO ACHIEVE BUSINESS VALUE | DELIVERING VALUE | Focus on projects and processes (and the people associated with them) while linking execution to strategy to deliver business value |

Too often, cybersecurity managers and their teams lack one or more of the critical capabilities and have difficulty finding ways to develop them. Bridging this gap requires an adaptive solution that re-examines traditional education; a program that is widely accessible, immediately relevant and nondisruptive to the participant's already busy schedule. Traditional programs for leadership development are either too concentrated (i.e. week-long leadership courses on a university campus or destination-education site) or too long, overly cumbersome and disjointed (i.e. traditional MBA programs). Research participants were clear in their responses about the need for a custom, targeted program focused on practical learning, not theoretical rhetoric. Ultimately, the vision is a leadership development program that is cost-effective, integrated, scalable, relevant and nondisruptive, and includes the following distinctive attributes.

| FACULTY | PROGRAM DURATION | INTENTIONAL DESIGN |
|---|---|---|
| Unparalleled perspective from industry-leading executives, educators and coaches | The 12-week program intentionally integrates participant learning with work | Weekly modules are integrated throughout the program to reinforce learning and application |
| **SIMULATION WEEK** | **LIVE EVENTS WITH CISOs** | **EXCLUSIVE WEBINARS** |
| After 10 weeks of content, Module 11 is a war gaming event for "real" application and review | CISOs lend "live" thought leadership every Friday | Exclusive webinars with CISOs and thought leaders are available to participants |
| **MANAGER INVOLVEMENT** | **NONDISRUPTIVE** | **THE LEARNING PLATFORM** |
| Supervising managers will receive dashboard reports that measure participant engagement and ROI | The 3–5 hours per week of content accommodates the busy schedules of security teams | The custom platform enables peer-based, social learning and networking to occur |

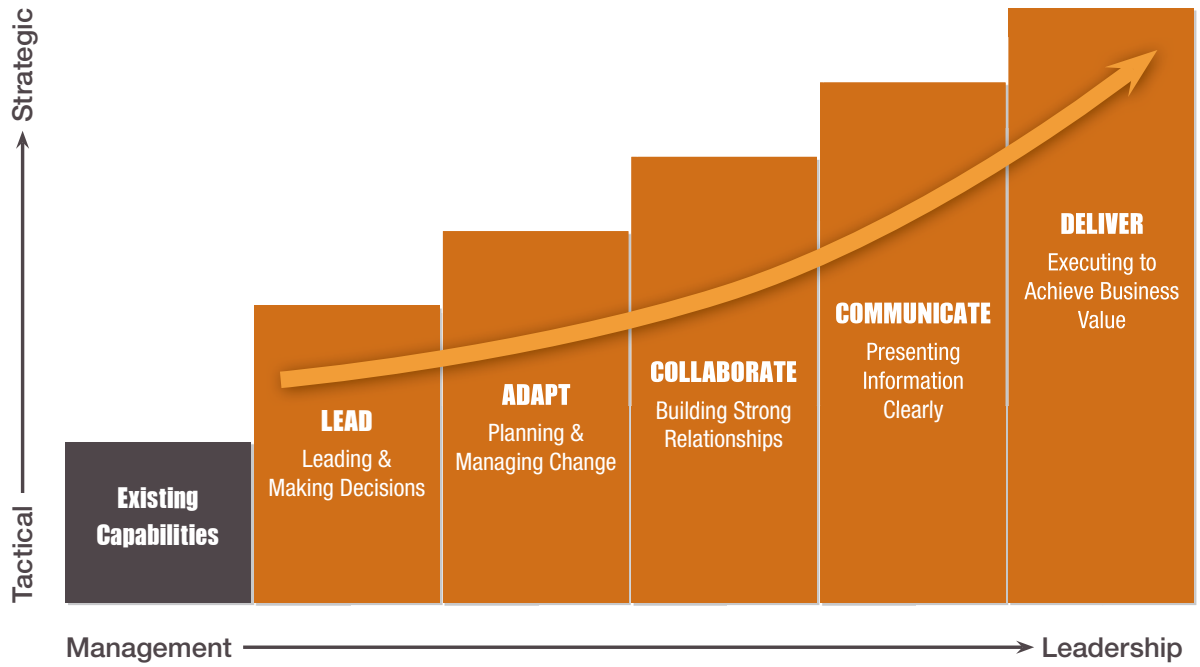
**The vision is a leadership development program that is cost-effective, integrated, scalable, relevant and nondisruptive.**

## THE LEARNING JOURNEY

### Content leverages existing abilities and (further) develops capabilities to lead, adapt, collaborate, communicate and deliver business value.

The following illustration depicts the "additive" nature of content and curriculum design. This is far different from traditional curriculum that is most often siloed, lacking integration in a holistic design.

### THE CAPABILITIES FRAMEWORK FOR CYBERSECURITY LEADERS



# PROGRAM MODULES

## MODULE 1: THE SECURITY LEADERSHIP MINDSET

This initial module contains a program overview focused on what it means to think and act as a cybersecurity leader – a business leader. It provides insights from members of the program's faculty on the ways in which leaders effectively identify and overcome challenging organizational and market conditions. This introductory material serves as the essential foundation to later integrate tools, practices, principles and protocols to achieve increasingly demanded business results.

Key Module Outcomes

- Demonstrate an understanding of the leadership mindset – it's about more than being a security professional, it's about being an enterprise business leader
- Create an Individual Development Plan to drive professional growth
- Identify opportunities for leadership improvement
- Begin cultivating a professional network of colleagues

## MODULE 2: THE ART OF SECURITY INTELLIGENCE

This module focuses on optimizing threat intelligence through a re-examination of traditional views on security. In the mercurial environment of cyber intelligence threats, shifting from a reactive stance toward a more dynamic proactive approach is essential to counter rapidly evolving tactics of cyberthreats. Leveraging a leadership mindset, participants delve into strategies for evaluating threat landscapes and implementing proactive defenses specifically catered to your unique organization.

Key Module Outcomes

- Switch from reactive to proactive defensive tactics and protocols
- Understand strategies for evaluation of threat landscapes and current risk practices
- Develop a flexible and effective security architecture

## MODULE 3: THE BALANCE BETWEEN SECURITY & INNOVATION

Building an effective information security organization is a balance between protecting and enabling. Finding the equilibrium between security control and innovation is a requirement in any enterprise. Security should be positioned as an enhancement to an organization, not an inhibitor. This module details the means by which industry-leading enterprises strike this balance, and in so doing, find ways to simplify complexity.

Key Module Outcomes

- Find a balance between security and efficiency
- Use security to enhance not inhibit innovation
- Understand the importance and means to simplify complexity

Program Modules Continued >

## MODULE 4: SECURITY CHANGE MANAGEMENT

While change is often dictated by strategic, financial or marketing considerations, the emphasis of this module is to prepare participants to engage in change initiated by others and to drive effective change as an active change agent. This module balances theoretical and pragmatic insights regarding how best to plan, lead and sustain organizational change. The specific practices detailed focus on the tactical aspects of a change framework and further examine the essential element of successful change: the people.

Key Module Outcomes

- Apply a proven framework for guiding organizational change
- Improve processes for defining the case for change, planning for change and sustaining change efforts
- Enhance ability to manage the practical and emotional aspects of change
- Improve capacity for employing inspirational communication when leading change

## MODULE 5: POSITIVE LEADERSHIP IN SECURITY

The way you show up as a leader matters. Instead of aiming for a state of normalcy or health, this module will focus on enabling leaders to create positively deviant performance. Positive leaders have the ability to constructively impact those around them. Through the four strategies of positive leadership (positive work climate, positive relationships, positive communication and positive meaning), participants will learn how they can be more positive leaders – thereby improving individual, team and organizational performance.

Key Module Outcomes

- Use positive leadership principles as individual and team performance indicators
- Improve leadership effectiveness through the application of positive leadership
- Employ the competing values framework to measure individual, team and organizational performance
- Create measurable action plans for performance improvement using the competing values framework.

## MODULE 6: COLLABORATION AND NEGOTIATION

Focusing on the Mutual Gains Approach to negotiations, this module emphasizes the collaboration necessary to produce superior outcomes, marked by efficient communication and extreme care for human relationships. Participants will learn how to best prepare, create value, distribute value and follow through within the context of negotiations.

Key Module Outcomes

- Create a plan to better prepare for negotiations
- Use creativity to create value within a negotiation
- Distribute value among negotiation parties
- Complete influence maps to identify stakeholders and increase effectiveness

## MODULE 7: SECURITY COMMUNICATION

This module focuses on adopting practical and meaningful techniques for how effective security leaders communicate within and outside of the organization. Participants will learn to how to effectively convey information across diverse stakeholder groups and business divisions to create awareness and make better decisions. Further, each participant gains an understanding of the contextual application of effective communication as it relates to leading others, diagnosing performance, providing and receiving feedback and leveraging human factors to improve performance.

Key Module Outcomes

- Execute a communication plan to better align tasks with team work
- Use emotion and logic to create win-win messaging
- Distribute individual and business value based on the method and content of communication
- Improve relationships and build stronger teams through communication

## MODULE 8: RELATIONSHIP MANAGEMENT

People matter. Everything we do and accomplish is grounded in our ability to work with and relate to others. Fostering relationships provides critical access to resources and networks of support. However, trusted relationships don't coalesce overnight; it is important to build relationships over time. In this module, participants will engage in strategies to create and sustain strong professional relationships and form critical partnerships.

Key Module Outcomes

- Understand that every single person in the organization is valuable and has a purpose
- Develop strategies to take care of your people, set and achieve high standards
- Create methods to balance the three fundamental components of a security system: people, policy and technology

## MODULE 9: SECURITY & THE NETWORK OF THINGS

With technological capabilities influencing increasingly larger portions of life, we benefit from the connectivity and compatibility of things. From our office to our cars, our home networks and health care devices, the network of things is becoming fundamental to our existence. To address risks within the network of things, we must understand the network of things. This module highlights trends, issues, concerns and solutions regarding networks necessary to develop and maintain effective risk management strategies.

Key Module Outcomes

- Broaden perspective (and clarity) of the Internet of Things to the network of things
- Understand the systems thinking relative to the network of things
- Know and be able to use the irrefutable laws of systems thinking

Program Modules Continued >

## MODULE 10: YOUR CHANGING ROLE IN SECURITY

With the growing threat of cyberattacks and data breaches, there is an increasing dependence on the skills of the cybersecurity leader. As a cybersecurity leader, you are uniquely positioned within an organization at the crux between IT values and business acumen. Creating an environment of accountability and personal responsibility, and striving to simplify complexity are essential soft skills for a cybersecurity leader. This module focuses on the changing landscape of security relative to the skills and capabilities required for a cybersecurity leader to act with confidence and generate business value.

Key Module Outcomes

- Simplify complexity by increasing communication and building confidence
- Translate far-reaching goals and missions into daily activities and behaviors
- Establish an environment of clarity of purpose, credibility and integrity
- Know the value and process of continuous learning

## MODULE 11: PERFORMANCE COACHING IN SECURITY

With unlimited time and resources, business proceeds as usual. However, no resource is unlimited, which means change and innovation must occur. By engaging in mock scenarios that emulate the marketplace, you can quickly assess your readiness. This module is designed to foster development and alignment within cybersecurity individuals and work teams through scenario-based drills, training and war games. NOTE: This module is a week-long facilitated simulation with daily live events/conference calls and may take up to three hours per day to fully engage.

Key Module Outcomes

- Asses team and organizational culture to determine leverage points of intervention to improve business results
- Improve relationships with stakeholders
- Use key business metrics as means for decision-making
- Implement drills, training and war games to asses capabilities and drive results

## MODULE 12: THE POWER OF ONE

From a systems thinking perspective, everything is connected. You and the work you do affects your team, enterprise, stakeholders, community and beyond. It is important to recognize the power and influence you have from a systems perspective as a cybersecurity leader. This capstone module leverages systems thinking to better understand the importance of how you show up and where you go from here.

Key Module Outcomes

- Your leadership rules
- Your oath of a leader
- Next steps on your leadership learning journey

# CURRICULUM MAP

| | | ASYNCHRONOUS | | | SYNCHRONOUS | |
|---|---|---|---|---|---|---|
| | | MONDAY | TUESDAY | WEDNESDAY | THURSDAY | FRIDAY |
| MODULE | THEME | OVERVIEW OF THEME AND PERSONAL REFLECTION | DETAIL OF THEME AND GROWTH OPPORTUNITIES | DETAIL OF THEME AND IMMEDIATE ACTION ITEMS | APPLICATION OF THEME AND PEER LEARNING | APPLICATION OF THEME AND COHORT REPORT OUTS |
| 1 | **THE SECURITY LEADERSHIP MINDSET** – Learning what it means to be an information security professional and business partner | Welcome from CISO and Module Introduction | Planning a Learning Community | Your Success Means Planning to Learn | Formula 1 Analogy and Team Case Study | Live Event with CISO |
| 2 | **THE ART OF SECURITY INTELLIGENCE** – Learning to optimize threat intelligence by shifting reactive reviews to proactive planning | Module Introduction | Threat Intelligence is a Process | Building Your Intelligence Plan | Formula 1 Analogy and Team Case Study | Live Event with CISO |
| 3 | **THE BALANCE BETWEEN SECURITY & INNOVATION** – Learning to minimize controls to leverage innovation and increase risk mitigation | Module Introduction | Technology Drives Enablement and Risk | Reducing Your Company Risk | Formula 1 Analogy and Team Case Study | Live Event with CISO |
| 4 | **SECURITY CHANGE MANAGEMENT** – Learning how best to plan, lead and sustain organizational change | Module Introduction | Leading Change is Hard Work | Measuring Change for Effectiveness | Formula 1 Analogy and Team Case Study | Live Event with CISO |
| 5 | **POSITIVE LEADERSHIP IN SECURITY** – Learning to enable the best of the human condition to increase engagement and performance | Module Introduction | Attributes of Positively Energizing Leaders | Strategies for Increased Engagement | Formula 1 Analogy and Team Case Study | Live Event with CISO |
| 6 | **COLLABORATION AND NEGOTIATION** – Learning the Mutual Gains Approach to negotiation as a way to minimize risk | Module Introduction | The Mutual Gains Approach to Negotiation | Bringing Value to the Business | Formula 1 Analogy and Team Case Study | Live Event with CISO |
| 7 | **SECURITY COMMUNICATION** – Learning how to speak the language of business and convey message across diverse stakeholders | Module Introduction | Speaking the Language of Business | Interpersonal Aspects of Effective Communication | Formula 1 Analogy and Team Case Study | Live Event with CISO |
| 8 | **RELATIONSHIP MANAGEMENT** – Learning how to build relationships that create better risk management | Module Introduction | People are Your Primary Perimeter | Your Relationship to Your People and the Business | Formula 1 Analogy and Team Case Study | Live Event with CISO |
| 9 | **SECURITY & THE NETWORK OF THINGS** – Learning to harness the power of your ecosystem as it becomes ubiquitously interconnected | Module Introduction | Harnessing the Power of Your Network | Risk Management Through Trust-Building | Formula 1 Analogy and Team Case Study | Live Event with CISO |
| 10 | **YOUR CHANGING ROLE IN SECURITY** – Learning the need for continuous learning and the integration of security and business acumen | Module Introduction | Attributes of the Next CISO and Security Team | Your Leadership Rules, Your Oath as a Leader | Formula 1 Analogy and Team Case Study | Live Event with CISO |
| 11 | **PERFORMANCE COACHING IN SECURITY** – Learning how to manage the complexity of reality through simulations and reviews | Module Introduction – War Game Simulation | Learning by Doing – War Game Simulation | Learning by Doing – War Game Simulation | Formula 1 Analogy and War Game Simulation | Live Event with CISO and War Game Simulation |
| 12 | **THE POWER OF ONE** – Taking accountability for the role as an information security professional and business partner | Module Introduction | Delivering Value to Your Business | It Only Takes One | Formula 1 Analogy and Team Case Study | Live Event with CISO |

## THE EVANTA ADVANTAGE

# The Professional Development Academy's CISO Community selected Evanta to collaborate with to develop the curriculum and facilitate this program. Evanta is a recognized leader in senior executive conference management, leadership education and community building.

The company hosts more than 200 events annually, the majority of which support the CIO, CHRO or CISO communities. The increasing pressure to develop front-line leaders was illuminated over years of working with these C-suite executives. With years of experience and demonstrated expertise in executive education, Evanta was the natural choice for this partnership.

Evanta was founded on the belief that collaboration is the key to shared economic prosperity. In an era of unprecedented technological, economic and global change, Evanta believes creating alignment between proven practices across disciplines is critical to long-term competitive advantage. This requires a new approach, one based on trust and cooperation between high-performance leaders to drive innovation.

Since their inception, all Evanta initiatives have been driven by practicing industry leaders. A tightly-governed, powerful network ensures the content and context of each of our programs remains pure and immediately applicable to real-world business issues.

**Online education can provide several advantages, including increased access and the ability to involve people. It also allows for the use of collaboration.**

**Glenda Rotvold & Sandy Braathen, University of North Dakota**

Evanta®

*We make leaders better.*

For more information, including a virtual tour of the Professional Development Academy, contact:

Dr. Tim Rahschulte
Chief Learning Officer
Evanta
tim.rahschulte@evanta.com
www.evanta.com/academy