15th Annual
OHIO INFORMATION SECURITY CONFERENCE

15th Annual OISC

Sinclair and AT&T Congratulate Hackathon Winners
Recipe for Success

By: Paul Moorman, IT Strategist, Catalyst Paper

Technology First is blessed with several successful special interest groups including the CIO Council, Women 4 Technology, Infrastructure and Data Analytics. It’s a simple recipe, but does require a lot of hard work, strong leadership and the dedication of quite a few people. So, while the following ingredients can’t guarantee success, it’s never a slam dunk.

First and foremost, each group is committed to delivering relevant content within their area of interest, and that’s the most difficult thing to get right. If content runs along too narrow a path, topics quickly run out, and it’s too broad, too few topics will be of interest to enough people. Finding that tricky balance takes time, listening to the group and making mid-course corrections. For example, the Data Analytics group has struck that balance very well, morphing from a business intelligence focus to the more cutting-edge data science, a wider topic area which in the last few years has exploded with topics in machine learning, artificial intelligence, blockchain and cloud-based services. Topic ideas are collected and voted on, with each group owning its own agenda and collectively deciding the frequency and timing of meetings.

With topics identified, each group solicits volunteers to lead sessions or help identify someone knowledgeable on the subject. This is normally a huge sticking point for most groups, but the group-directed agenda significantly increases people’s desire to share their knowledge and they have the industry contacts helpful to identify external speakers. These sessions are informal and very interactive, a friendly environment to seize your chance with the mic. Further, the opportunity to network with your industry contacts helpful to identify external speakers. These sessions are informal and very interactive, a friendly environment to seize your chance with the mic. Further, the opportunity to network with your peers, share advice and gain their perspectives is equally valuable.

The final keys are the group’s leadership and the behind-the-scenes support. The leaders are those individuals with a passion for group purposes and are skilled in keeping the ideas, voting and topic timing of meetings.

Women 4 Technology, Infrastructure and Data Analytics. It’s a simple recipe, but does require a lot of hard work, strong leadership and the dedication of quite a few people. So, while the following ingredients can’t guarantee success, it’s never a slam dunk.

First and foremost, each group is committed to delivering relevant content within their area of interest, and that’s the most difficult thing to get right. If content runs along too narrow a path, topics quickly run out, and it’s too broad, too few topics will be of interest to enough people. Finding that tricky balance takes time, listening to the group and making mid-course corrections. For example, the Data Analytics group has struck that balance very well, morphing from a business intelligence focus to the more cutting-edge data science, a wider topic area which in the last few years has exploded with topics in machine learning, artificial intelligence, blockchain and cloud-based services. Topic ideas are collected and voted on, with each group owning its own agenda and collectively deciding the frequency and timing of meetings.

With topics identified, each group solicits volunteers to lead sessions or help identify someone knowledgeable on the subject. This is normally a huge sticking point for most groups, but the group-directed agenda significantly increases people’s desire to share their knowledge and they have the industry contacts helpful to identify external speakers. These sessions are informal and very interactive, a friendly environment to seize your chance with the mic. Further, the opportunity to network with your peers, share advice and gain their perspectives is equally valuable.

The final keys are the group’s leadership and the behind-the-scenes support. The leaders are those individuals with a passion for group purposes and are skilled in keeping the ideas, voting and topic timing of meetings.

Simple, yes. Easy, no. Nothing this good is ever easy.
Ransomware: Putting a Stop to IT's Greatest Current Challenge

By: Karen Greer, Senior Content Technologies and Matthew Phillion, Sophos

The industry certainly has a talent for naming things: ransomware, the greatest current challenge for IT professionals today, as we sense during our campaigns. The ability to take over a user’s data or machine, encrypting decryptable documents until a ransom is paid — and sometimes not even then, as there’s no known remedy there — has to cause the following catastrophic: learn to everyone from billion-dollar enterprises to your grandma opening up the wrong email at her kitchen table.

2017 was a brutal year for ransomware, with indications trending upward from 2016, which was already the worst year for ransomware on record. Organizations were hit with two headline-making ransomware attacks — May’s Wannacry/WannaCry attack followed by June’s NotPetya attack — but it wasn’t just the worldwide news, news-making attacks that were the problem.

No one is immune. Various studies show that healthcare and financial services businesses are the top two targets for ransomware. In fact, 92% of IT firms reported ransomware attacks on their clients. In some ways we don’t know how bad the problem is: despite these numbers, only one in ten companies are actually reported.

And paying off the cybercriminals doesn’t help. The FBI also notes that 39% of businesses who paid the ransom were attacked again later. Experts believe this is because organizations who pay out have identified themselves as businesses both with data of value, and data they are willing to pay for.

What can we do to stop ransomware?

Early on, there was a push toward backing up critical data — after all, if you had a backup of encrypted files, you needed to get those files back, logic dictated. But that wasn’t completely effective, and carried with it additional risks, such as not backing up often enough, or losing your backup files in general. Stopping ransomware needs to be about prevention, proactive rather than reactive.

Traditional antivirus solutions are not without value, but for risks like ransomware attacks, those traditional prevention methods, relying on signatures to detect known malware, fall far short. No matter how many antivirus updates you install, and scans how many files you run, there is always the chance that your signature database isn’t as up to date as the attacker.

One note on automation

A ransomware attack can cripple a business with incredible speed, so the more automated the security response, the better. An attack can happen at any time, to any user. Having solutions that can identify malicious, unusual, or questionable behavior and stop it, preventing further damage until the humans charged with keeping the organization and its users safe can be alerted, is pivotal in a threat landscape that evolves in seconds, not weeks.

Not only that, but having technology that works on multiple levels — watching for unapproved encryption, the use of exploits, and more, without the need of a human hand and command those preventative and defensive measures, means if an administrator can actually sleep at night knowing their users and data are protected under automated, ever-vigilant protection.

The human error factor can’t be discounted here, as well. The smartest end user in the world is still capable of falling victim to an attack. Research has shown that users open phishing emails and other fake messages at higher rate than they do actual marketing or advertising emails — and this isn’t indicative of the intelligence of the end user, but rather shows how skilled the bad guys have become at crafting messages users will believe. This adds to the pressure to have automated, intelligent protection.

Educing your end users on what to look for and what to do, or more importantly, not to do, in the case of a malware attack can narrow your organization’s largest attack vector.

Solid and user education side by side with powerful, automated, next-gen ransomware prevention can truly build up powerful suit of armor against the ever-changing online threat landscape.
“The Future of Cyber-Autonomy”

My vision is to automatically check and defend the world’s software from exploitable bugs. In order to achieve this vision, I am building technology that shifts the attack/defend game away from the current manual approaches for finding and fixing software security vulnerabilities to fully autonomous cyber reasoning systems.

In this talk, I will describe the DARPA Cyber Grand Challenge, the first effort to create a fully autonomous cyber security system. I’ll focus on Mayhem, built by ForAllSecure. Mayhem can find new vulnerabilities, generate exploits, and self-heal off-the-shelf software. Mayhem is the result of 10 years of academic research and 2 years of commercial development. Mayhem competed and won a $2 million dollar prize in the US Cyber Grand Challenge competition co-hosted at DEFCON 2016.

I will describe how Mayhem works, the Cyber Grand Challenge competition, and how Mayhem fared against the world’s best hacking teams. I will also describe how Mayhem, and other autonomous systems like it, will change the security landscape in the next decade.

“An Attacker’s Perspective”

Dave’s presentation is a journey through the “eyes of an attacker” as he sets the stage for attacking 2 large industry verticals – retail and healthcare.

He provides insight into:
- The decision space of today’s attackers and their monetization cycle.
- How attackers familiarize themselves with a target space without ever touching the target network.

His presentation will include a variety of techniques companies can use to curtail tried-and-true techniques to reduce an attacker’s return on investment.
Breakout Sessions

Engaging Millennials & Gen Zs in Cybersecurity: Who Are They & How Do You Move Them From ‘Always Connected’ to ‘Awesomely Secured?’

Kevin Carpenter, Director, RSM USA LLP

Technology First | March 2018

Apolonio “Apps” Garcia, CEO, HealthGuard

Dr. Devesh Kaushik; Gary Warzala, CISO, Fifth Third Bank; Gary Warzala; John S. Bommer, Jr.

Millennials and “Gen Zs” are poised to dramatically impact the global workforce over the next few years as they meld together personal and professional lives with “always connected” technologies and applications. These changes will pose serious challenges to current corporate structures and organizational boundaries and will drive the need for protection in the ways that these generations view technology, privacy, and cybersecurity. and offer preliminary results & lessons learned regarding effective ways to impact attitudes and behaviors through (U.S.) cyber resilience engagement methodology.

Tom Skill; James Robson; Jamie Luckett; Abbi Papenheim – Dayton University

Incorporating Cybersecurity into Industrial Automation and Control Systems

Incorporating Cybersecurity into Industrial Automation and Control Systems (IACS) requires a holistic defense-in-depth approach. This discussion will include Cybersecurity Cybersecurity standards, trends, case studies, and system-level conformance with the attack context identity, priority, location, and impact. Attendees will better understand how IACS often require specialized Cybersecurity requirements and how to take advantage of these tools.

Michael Vucetic, Connected Services, Rockwell Automation

Stealing Domain Admin (or How I Learned to Stop Worrying and Love the CSSF)

This presentation will walk you through a penetration tester’s process, step-by-step, as the tester goes from unauthorized outsider to domain admin (without being detected).

Jerod Brennen, Security Architect, One Identity

Do0 Requirement Toolkit for Manufacturers

Small to medium sized manufacturers struggle with assessing their new DoD regulations. While these companies focus on staying competitive within the civil and military supply chains, regulations require them to address the security of their supply chains. This toolkit will provide manufacturers guidance on assessing risk, determining control requirements, and selecting tools to implement effective controls. This self-contained toolkit provides a user-friendly method for creating and monitoring risk profiles for manufacturers interested in compliance.

Daniel Cleaver; Dr. Naasen Said – University of Cincinnati Information Technology Solutions

Using Threat Intelligence to Improve Risk Management

Cyber threat intelligence is becoming more pervasive, valuable, and sophisticated. While traditional risk management practices are still vital, new tools and techniques can greatly enhance an organization’s defense-in-depth approach. This discussion will include the treatment of risk and threat intelligence, identifying threats, and managing the impact. In this discussion, CenturyLink will describe how to turn intangible threat data into a powerful threat management service and how to take advantage of it.

Michael Smith, Senior Director of Security Solutions, CenturyLink

Is RWF Worth the Cost?

In a cybersecurity world filled with compliance mandates we have researched the costs being imposed. The benefit of the NIST 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, to determine which controls are more valuable for an organization to implement when it comes to defeating or adversary’s workload. Our research will provide evidence of the financial advantage, or disadvantage of implementing specific security controls. Included in this presentation is insight into our customized risk-based scoring process using the NIST Revit scoring model.

Rebecca Oronochnich; Jeff Hughes – Technical University of Delft

Cybersecurity in the Supply Chain

In this presentation, I want to outline the importance of Cybersecurity measures taken in the supply chain. Major breaches like the Target breach in 2013 were caused by heavily integrated supply chains. This resulted in increased access to critical infrastructure. Now that organizations have received the damage, it is likely to happen again.

Thomas Runge; Partner, Gritia

Security Threats Don’t Discriminate. Learn how any size IT department can tackle today’s - and tomorrow’s - threats.

While security measures for IT departments of any size and budget aren’t increasing at the same rate, b&bre;nt, Network Operations Manager for Comcast/Care Family of Companies; Nick Trifiletti, Barracuda

Regional Cyber Workforce Development

Regional (S)IoH activities to promote cyber education, training and workforce development and the potential role the OISC attendees could take.

Damon Harber; President and CEO, Ventis Global Investigations

Policy Changes for Cybersecurity Deterrence

At times, we are faced with a situation where an interaction occurs in the cybersecurity realm without any legal oversight. In cybersecurity, the interactions between customers and providers are targeted and challenged by nation states that intentionally exploit the lack of legal authority to provide retribution and deterrence in cyberspace. Therefore, I posit that cyberspace letters of marque and reprisal and international maritime law could be beneficial to the cybersecurity community.

Tom Kopchak; Steve McMaster - Hurricane Labs

Blockchain: Preparing for Disruption

Structural: What is Blockchain and how does it impact companies in the coming years. This presentation will review blockchain and blockchain technologies and talk about how they will disrupt business. This talk will also cover implications for using current blockchain technologies to improve security and privacy.

Kevin Carpenter, Director, RSM USA LLP

Conducting an Incident Response from a Forensics Standpoint

Learn methodologies and techniques for conducting an incident response from the perspective of a forensics examiner. Explore the necessity of preserving evidence, tools & techniques for analyzing and interpreting forensic artifacts, and how to work together. Understand the Legal, Business, and Practical implications of performing an incident response. Learn how to Preserve and Analyze crucial forensic evidence, Gather Tips, Tricks & Tools when conducting an Incident Response.

Damon Harber; President and CEO, Ventis Global Investigations

The People Problem: Examining the Weakest Link

It’s often alluded that the greatest bane to security is the user. The people that interface with our information systems are mostly referred to as the weakest link. Technological advancements attempts to compensate for these weaknesses, yet social engineering is the keystone of the most common methods of attack. The truth is, there is a people problem in information security, a really big one... but it’s not the user.

Dan Collins, Senior Risk Consultant

Supercharged SIEM: Empowering your logs with the right data

How do you decide what log sources to focus on to help allocate these resources when designing your security program? If you want useful alerts, you need to get the right data. In this presentation, Tom and Steve will walk you through how you identify the security use case that is most practical to your organization, as well as the log sources that are beneficial to include in any SIEM environment. Our information is backed by a variety of real-life examples and from experiences we’ve had in designing security solutions for our clients.

Tom Kopchak; Steve McMaster - Hurricane Labs

Incorporating Cybersecurity Into Industrial Automation

Incorporating Cybersecurity into Industrial Automation and Control Systems (IACS) requires a holistic defense-in-depth approach. This discussion will include IACS cyber security threats, standards, case studies, and system-level conformance with the attack context identity, priority, location, and impact. Attendees will better understand how IACS often require specialized Cybersecurity requirements and how to take advantage of these tools.

Michael Vucetic, Connected Services, Rockwell Automation

Breakfast Keynote:

This presentation will walk you through a penetration tester’s process, step-by-step, as the tester goes from unauthorized outsider to domain admin (without being detected).

Jerod Brennen, Security Architect, One Identity

Do0 Requirement Toolkit for Manufacturers

Small to medium sized manufacturers struggle with assessing their new DoD regulations. While these companies focus on staying competitive within the civil and military supply chains, regulations require them to address the security of their supply chains. This toolkit will provide manufacturers guidance on assessing risk, determining control requirements, and selecting tools to implement effective controls. This self-contained toolkit provides a user-friendly method for creating and monitoring risk profiles for manufacturers interested in compliance.

Daniel Cleaver; Dr. Naasen Said – University of Cincinnati Information Technology Solutions

Using Threat Intelligence to Improve Risk Management

Cyber threat intelligence is becoming more pervasive, valuable, and sophisticated. While traditional risk management practices are still vital, new tools and techniques can greatly enhance an organization’s defense-in-depth approach. This discussion will include the treatment of risk and threat intelligence, identifying threats, and managing the impact. In this discussion, CenturyLink will describe how to turn intangible threat data into a powerful threat management service and how to take advantage of it.

Michael Smith, Senior Director of Security Solutions, CenturyLink

Is RWF Worth the Cost?

In a cybersecurity world filled with compliance mandates we have researched the costs being imposed. The benefit of the NIST 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, to determine which controls are more valuable for an organization to implement when it comes to defeating or adversary’s workload. Our research will provide evidence of the financial advantage, or disadvantage of implementing specific security controls. Included in this presentation is insight into our customized risk-based scoring process using the NIST Revit scoring model.

Rebecca Oronochnich; Jeff Hughes – Technical University of Delft

Cybersecurity in the Supply Chain

In this presentation, I want to outline the importance of Cybersecurity measures taken in the supply chain. Major breaches like the Target breach in 2013 were caused by heavily integrated supply chains. This resulted in increased access to critical infrastructure. Now that organizations have received the damage, it is likely to happen again.

Thomas Runge; Partner, Gritia

Security Threats Don’t Discriminate. Learn how any size IT department can tackle today’s - and tomorrow’s - threats.

While security measures for IT departments of any size and budget aren’t increasing at the same rate, b&bre;nt, Network Operations Manager for Comcast/Care Family of Companies; Nick Trifiletti, Barracuda

Regional Cyber Workforce Development

Regional (S)IoH activities to promote cyber education, training and workforce development and the potential role the OISC attendees could take.

Damon Harber; President and CEO, Ventis Global Investigations

The People Problem: Examining the Weakest Link

It’s often alluded that the greatest bane to security is the user. The people that interface with our information systems are mostly referred to as the weakest link. Technological advancements attempts to compensate for these weaknesses, yet social engineering is the keystone of the most common methods of attack. The truth is, there is a people problem in information security, a really big one... but it’s not the user.

Dan Collins, Senior Risk Consultant

Supercharged SIEM: Empowering your logs with the right data

How do you decide what log sources to focus on to help allocate these resources when designing your security program? If you want useful alerts, you need to get the right data. In this presentation, Tom and Steve will walk you through how you identify the security use case that is most practical to your organization, as well as the log sources that are beneficial to include in any SIEM environment. Our information is backed by a variety of real-life examples and from experiences we’ve had in designing security solutions for our clients.

Tom Kopchak; Steve McMaster - Hurricane Labs

Technology First | March 2018

Incorporating Cybersecurity Into Industrial Automation and Control Systems

Incorporating Cybersecurity into Industrial Automation and Control Systems (IACS) requires a holistic defense-in-depth approach. This discussion will include IACS cyber security threats, standards, case studies, and system-level conformance with the attack context identity, priority, location, and impact. Attendees will better understand how IACS often require specialized Cybersecurity requirements and how to take advantage of these tools.

Michael Vucetic, Connected Services, Rockwell Automation
Conference Instructions

Conference Mobile Website

As an attendee, using the browser of your choice you can visit https://2018oisc.sched.com on your smartphone or desktop to locate the conference website. If you pre-registered for the event, your email has already been entered into the system so you just need to log in and create a password of your choosing. If you did not pre-register, you can still use the website to get details on the sessions and schedule.

Your Schedule for the Day

Once you are logged in we encourage you to visit the “expanded” version of the schedule to read through the various sessions available to you. If you find the speaker/topic that you plan to attend in each session, just click the circle next to “Add to My Sched” and this will start to build your agenda for the day.

Virtual Business Card

Now this year! Your name badge has a unique QR code with (only) your name, company, position and email. Should you wish to share this information with another conference attendee or exhibitor, simply download the BadgeScan app (Apple or Android) and then scan that person’s QR code. You can also update your own information to include more information such as telephone number or website. This information is ONLY available to the people you choose to share it with.

Your Feedback

For future use, please note that each session has a feedback survey button. Once you have attended the session we ask that you provide your review of the presentation. The feedback will help the speakers and Technology First build a better conference next year. There is also an evaluation for the Overall Conference Experience that we hope you will complete at or near the end of the day. We will provide this information to the conference committee for next year’s planning.

We believe
the digitally connected enterprise can outperform.

See what’s changing.
enterprise.spectrum.com/webelieve

©2018 Charter Communications. All Rights Reserved. Not all products, pricing and promotions available in all areas. Subject to Change. Without notice. All trademarks shown are property of their respective owners.
BUSTED!

By: Diana Tuilio, Business Technology Strategist, Alleron

"The greater our knowledge increases the more our ignorance unfolds." - Isaac Bashevis Singer

Why is it that we believe not knowing everything is a sign of weakness? Who actually knows everything? Sound crazy, but this is something that I hear from people. People that are smart, accomplished, and successful. I've been susceptible to healing this way myself at times.

Take this situation for example

You are called in for an interview for a job that you really want. You read through the job description, and you know in your heart that you have the experience and knowledge to rock it. Man, this job is perfect for you! The day of the interview, you are a nervous mess. You sweat waiting for your name to be called to talk with the interviewer. You say to yourself, “Why on Earth did I fool myself into thinking I could bluff my way through this interview? Why do I think this person wants a ‘fake and bolts me on it’?” You make it through the interview... barely. No one arrested you for falsifying your experience or knowledge, but you still have a lingering feeling that you pushed yourself beyond your rights to do for this great opportunity.

I know that I have been in this situation before. What about you? You may have gotten the job and felt that you “pulled it off,” or you may not have gotten the job and felt that the interviewer saw through you but was too polite to tell you in person. If you didn’t get it, it is possible, you were qualified, but you didn’t seem committed to wanting to make the change to the role that the hiring manager was looking for?

I recently had lunch with a very talented person that has a ton of experience and knowledge in a highly sought-after skill set and industry. This individual talked with passion about his work, and he showed a love of learning and self-motivation that gained him invaluable experience that any company would love to have in their organization. His lunch date went on to tell me that he wanted to grow and take on more responsibility in another organization, but...

I was stumped by this abrupt change in demeanor. When I asked him about his hesitation, he said he was terrified that someone would see through him and realize that a current employer can vouch for easily if they realize that promoting great talent is one with:

• The desire to make the company better through efficiency and effectiveness by
• Ambition to take on more responsibility?
• A proven track record for a passion to learn and experience?
• Enough experience and training in the targeted role to be effective but maybe not an
• A cultural fit, and an effective collaborator that pulls out the strengths of teammates
• Ambition to take on more responsibility?
• A proven track record for a passion to learn and experience?
• Discounting candidates that have proven their passion for learning and applying themselves suitably in previous roles but don’t exactly fit your job description
• Getting candidates that are afraid to show their true capabilities in interviews with you
• Retaining employees that should move on to grow their talent even if it is not with you
• Not sharing your ideas that make you stand out and could make a difference in
• Beginning to dread going to work in your current workplace
• Being stuck in a job that is no longer challenging or helping grow you into your next

There are so many things that are concerning about a potential epidemic of self-doubt in the workplace. After being on both sides of the interview table, I can see the potential damage from the perspective of the professional and the potential employer:

Qualified Professional

• Being stuck in a job that is no longer challenging or helping grow you into your next
• Not even attempting to pursue a role because you don’t think you meet the
• Thinking that there will never be a time that your knowledge and experience will be
• Getting candidates that are afraid to show their true capabilities in interviews with you
• Retaining employees that should move on to grow their talent even if it is not with you
• Not sharing your ideas that make you stand out and could make a difference in
• Beginning to dread going to work in your current workplace
• Being stuck in a job that is no longer challenging or helping grow you into your next

Potential Employer

• Not getting the best candidates to apply for your needed roles
• Ambition to take on more responsibility?
• A proven track record for a passion to learn and experience?
• Enough experience and training in the targeted role to be effective but maybe not an
• A cultural fit, and an effective collaborator that pulls out the strengths of teammates
• Ambition to take on more responsibility?
• A proven track record for a passion to learn and experience?
• Discounting candidates that have proven their passion for learning and applying themselves suitably in previous roles but don’t exactly fit your job description
• Getting candidates that are afraid to show their true capabilities in interviews with you
• Retaining employees that should move on to grow their talent even if it is not with you
• Not sharing your ideas that make you stand out and could make a difference in
• Beginning to dread going to work in your current workplace
• Being stuck in a job that is no longer challenging or helping grow you into your next

It takes more work to vet out those types of qualities in a candidate. These are not things that jump off the page of the resume. They are things that can be expressed by a confident candidate and drawn out by a curious interviewer. They are also things that a current employer can vouch for easily if they realize that promoting great talent whenever they may be going is good for everyone involved.

Some of the best talent in the marketplace may not fit the automatic screening filter on the resume application. That is a great shame, but it is encouraging for us to look beyond the exact words in the job description and to be inevitably curious about our prospects. I will leave you with these two insightful quotes on curiosity and experience.

“I have no special talent. I am only passionately curious.” - Albert Einstein

“Be brave. Take risks. Nothing can substitute experience.” - Paulo Coelho

Sinclair Community College and AT&T congratulate Hackathon Winners

Sinclair Community College and AT&T hosted the finale of the Miami Valley Teen Hackathon on January 31st, which was the culmination of a 12-week coding and technology contest for Miami Valley high school students. Students created projects to secure the home of the future using state-of-the-art technology. The work of the student teams was judged on quality, the potential impact on the Miami Valley region, execution, and creativity. The students entered projects in one of the four following categories: Apps and Coding, Robotics, Cybersecurity and, UAVs and Drones Technology.

The following schools placed first in the competitions

• Miami Valley CTC - Apps & Coding
• Miami Valley CTC - Robotics
• Kings High School - Cybersecurity
• UAVs & Drones - Hamilton High School

The Miami Valley Teen Hackathon was designed to equip high school students with 21st century skills via computer science education, provide college and career readiness, solve real-world problems, and open the doors of opportunity and creativity.

“One of the major workforce development questions today is how to fix the tech talent shortage,” said Steve Johnson, President, Sinclair Community College. “Colleges and companies must partner to introduce non-traditional methods to stimulate interest and talent in tech fields. The Miami Valley Teen Coding Challenge is one way in which AT&T and Sinclair Community College and the Miami Valley Tech Prep Consortium are working together to promote computer science and technology education, prepare high schools for college and careers, and enable them to express their creativity.”

“By encouraging students to learn how to code and apply technology, we are spotlighting the enormous demand for developers and engineers needed to create the software that will drive the internet of things, smart cities, and our mobile economy,” said Mark Rebbert, External Affairs Director, AT&T Ohio.

23 teams from 14 area high schools participated in the Hackathon. Members of the winning teams received home automation prizes.
Technology First would like to thank and recognize its Board of Directors. They provide input into the strategic direction of the organization and actively lead working committees that drive our programs and services.

<table>
<thead>
<tr>
<th>Name</th>
<th>Title/Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marcia Albers</td>
<td>Executive Director, Technology First</td>
</tr>
<tr>
<td>Diana Bolden</td>
<td>Former CIO, Teradata</td>
</tr>
<tr>
<td>Jim Bradley</td>
<td>CHAIR, Global IT Vice President, Teconet</td>
</tr>
<tr>
<td>Gary Codoluppi</td>
<td>Vice President, Marketing and Business Development, Ross Group DBMA</td>
</tr>
<tr>
<td>Doug Couch</td>
<td>Vice President, Information Technology Services, Speedway</td>
</tr>
<tr>
<td>Tim Ewart</td>
<td>Technical Director, Air, Space and Cyberspace Directorate, HQ Air Force Command</td>
</tr>
<tr>
<td>Pat Garland</td>
<td>Vice President, IT CareSource</td>
</tr>
<tr>
<td>Treg Gilstorf</td>
<td>Senior Director of IT, Yaikawa Motoman</td>
</tr>
<tr>
<td>Gary Ginter</td>
<td>System Vice President, CIO Premier Health</td>
</tr>
<tr>
<td>Bryan J. Hogan</td>
<td>President / CEO, AhdencIT</td>
</tr>
<tr>
<td>John Huelusman</td>
<td>Director of Business Support Solutions, HUB</td>
</tr>
<tr>
<td>Tim Hull</td>
<td>Director, Bitstorm Connect, Think Patented</td>
</tr>
<tr>
<td>Scott McCollum</td>
<td>Chief Information Officer, Sinclair Community College</td>
</tr>
<tr>
<td>Monique McGlinch</td>
<td>VP, Information Technology &amp; Proj Mgt Office, MidMark</td>
</tr>
<tr>
<td>Dave Mezera</td>
<td>President, DataVard</td>
</tr>
<tr>
<td>Paul Moorman</td>
<td>IT Strategist, Catalyst Paper</td>
</tr>
<tr>
<td>Shu Schiller</td>
<td>Associate Professor and Chair Information Systems and Operations Management, Wright State University</td>
</tr>
<tr>
<td>Thomas Skill</td>
<td>Associate Provost &amp; CIO, University of Dayton</td>
</tr>
<tr>
<td>Diana Tuttle</td>
<td>Business Technology Strategist, Akerson</td>
</tr>
<tr>
<td>Jeff Van Fleet</td>
<td>President, Lighthouse Technologies</td>
</tr>
</tbody>
</table>

Writers: Our mission is to support the growth of Greater Dayton’s information technology industry. Technology First provides a forum for educators, business, and technical professionals to communicate their expertise and lessons learned while working in the field. Please submit the article in Word, preferably with 500 to 700 words, with any graphics in pdf to malbers@technologyfirst.org. Please include your name, business organization, business address, phone number, fax number, e-mail address, and a brief description of any professional accomplishments. Please also include a digital photograph if available.

Subscriptions: Non-member business/home delivery of this publication is available at $120/year (11 issues). Mail name, address and check made payable to Technology First.

2018 Technology First. All rights reserved. Technology First | March 2018

Technology First | March 2018
Meet your challenges when they’re still opportunities.

RSM and our global network of consultants specialize in working with dynamic, growing companies. This focus leads to custom insights designed to meet your specific challenges. Our experience, combined with yours, helps you move forward with confidence to reach even higher goals.

rsmus.com/technology

YOUR MISSION IS CRITICAL.
THAT’S ALL WE THINK ABOUT.

Your mission depends on data and computing power being available without fail. Vertiv, formerly Emerson Network Power, has a laser focus on delivering vital, innovative and intelligent applications for high-tech environments. We create value for our customers by making your critical mission our own.

Liebert® Trellis™

Represented locally by Uptime Solutions
www.uptime-inc.com
937-237-3400

Digital is not the flavor of the day. It’s the essence of tomorrow.

Whether your project is practical or extreme, we have developers & designers who know technology and can boost your customer engagement.

CALL TODAY to get a free quote to bring that idea to life.
937.221.2700 or marsha.martin@taylordigital.io

www.taylordigital.io

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING