Good morning.

I want to start my presentation by expressing my very sincere thanks to Tom Kohler and the entire team who put together the Command and Control Conference. It is my distinct honor and privilege to speak with all of you today.

I am fortunate to be invited to speak at many conferences around the world, but this conference is distinctly different from many others. The Command and Control conference not only covers an exceptionally wide range of critical issues, but it goes further by moving those of us we who are attending to do more than simply becoming more aware of the issues, we are moving to action.

This is precisely the sort of event we need in the face of the ever-expanding cyber security threats we face and which will be the focus of my discussion today.

I would be remis however, if I didn't confess that there was a small part of my agreeing to come to Munich and speak with you today that includes the fact that this will enable me to attend my very first Octoberfest events here in Germany. We do imitate Octoberfest in the United States but I'm quite sure that being here in Germany especially at this time will be an especially enjoyable event for me personally and so again, thank you for inviting me.

In the United States we have a somewhat different – and to be honest less enjoyable – October tradition. In the USA October is officially National Cyber Security Awareness Month.

Cyber Security Awareness month was a tradition started in the US about nearly 20 years. I have been in this field dating back to this era and I can tell you that back then, when the Internet was just becoming widely available, everyone just assumed it was secure.

How times have changed!

Back then people who had heard about this cyber security problem assumed that it was something like the Y2K non-event that occurred at the turn of the century. For those of you not old enough to know what Y2K was -- it was a scary story suggesting that since computers had not programed the switch from the 1900s to the 2000 properly all the computers were going to crash. Obviously, that did not happen, and a simple operational fix resolved any problem that might have occurred.

The cyber security threat is nothing like the Y2K problem, yet too many people are still assuming that there will be some simple operational fix, a new software, or government regulation that will quickly and effectively solve the cyber security problem.

I'm here to assure you, that will not be the case.

So while we have, in the last 20 years, achieved substantial awareness of the cyber security problem, but what we have failed to fully achieve is **understanding** of the cyber threat

That lack of true understanding of the issue has largely prevented us from creating the effective, comprehensive and internationally collaborative programs we need-
to address the issue.

I could spend the entire speech describing the cyber security problem, but I won't. Suffice to say that by even modest estimates, (SLIDE 2) in the roughly 2 minutes it has taken me to get to this point in the speech cyber criminals stole more than 5 million Euros. 12,000 identities were stolen and nearly 2000 new versions of mal-ware were created – that's what happens every 2 minutes on the Internet every day. And these numbers are expected to double again by 2020, and triple by 2030.

To put this in a national security the US Secretary for Homeland Security Kiersten Neilson believes that in 2018 the security threats from cyber now are greater than threats from international terrorism or any other physical attack method.

The threat cyber poses to our economy, our personal privacy, our physical safety and the very democratic process we life under, has been amply demonstrated.

And now the bad news.

Things are likely to get much worse, much worse. There are several reasons things are likely to get worse.

First is the fact that our cyber networks are inherently insecure – and growing weaker by the day. (SLIDE 3)

The Internet was never designed to be secure in the first place. It was designed to be an open system. In fact, if you ask the people who originally designed about why this is the case some of them will tell you "we were just trying to pass back and forth some research papers. We didn't intend for you to run the entire world on this system. " But that is what has actually happened.

In addition, since virtually no one writes code from scratch, the vulnerabilities of the all the original protocols are carried over into the new modifications we make to the system like smart phones, tablets and the Internet of things which only compounds the technical vulnerability of the entire system.

Moreover, it turns out the attack community are pretty smart business people and have wisely taken substantial portions of the billions of dollars they are netting from cybercrime and reinvesting it in their business, so they are finding all new weaknesses and vulnerabilities we didn't even know about.

Not only are they good business people, they are getting technically more sophisticated. The "common" cyber-attack of 2018 would have been considered an ultra-sophisticated attack just a few years ago. (SLIDE 4)

In fact, a decade ago the term APT was coined which stood for "the Advanced Persistent Threat." These APT attacks referred to the sophisticated methods available then only to the military. These elite attack methods were multi-level, staged attacks that include "designer-malware" targeted specific individuals, not just networks, and use personal recognizance to compromise innocent insiders often breaching distant points in networks to gain access to sensitive data father in the network.

Today, we see these same techniques being used commonly in the cybercrime world – sometimes by nation states or their affiliates and sometimes by "common" criminals. It's not just the government, or the defense industrial base and the financial sector that experiences these sophisticated attacks;

they are now launched against utilities, manufacturers, retailers, universities and even movie studios.

The APT – the Advanced Persistent Threat --has now become the Average Persistent Threat.

But it's not just that the system is weak and getting weaker -- and the attackers are sophisticated and getting better – much better. The more endemic problem is economic. The reality is that in cyber security, virtually all the economic incentives favor the attacker. (SLIDE 5)

Put simply this is the economic balance of cyber security is this: Cyber-attacks are inexpensive and easy to acquire. They are enormously profitable. The business model is excellent, and attackers are often extensively resourced – increasingly with nation state assistance

On the defense side we are defending an inherently porous system. Attackers have a first mover advantage. It's hard to demonstrate ROI to things that are prevented, which mitigates against adequate investment. We do not have a coherent international legal framework with which to address the issue. Furthermore, our excellent law enforcement personnel are drastically under resourced leading to the sad fact that we successfully prosecute maybe 1 or 2 % of cyber criminals.

Perhaps the most pernicious aspect of our failure to properly understand the cyber issue, is that it leads to a simplistic, blame the victim, narrative.

In this narrative the main problem is that we have a bunch of lazy, greedy, and stupid people managing our cyber security and as a result we always are able to discover that there was

some simple practice, standard or patch that, with proper attention, could have/should been deployed which would have prevented the attack.

While these narrative plays to the public, , it belies a gross misunderstanding of what we are dealing with.

Worse, it leads to blaming the victims of cyber-attacks and the promotion simplistic solutions often built around the notion that if we simply punish the victims of cyber-attacks more harshly they will magickly find a way to protect us. If we are told cyber breaches are the fault of one stupid lazy or corrupt person, then the answer is stiffer penalties.

Now I'm not saying that we don't have some stupid, lazy greedy people in our institutions, I'm sure we do. What I'm saying is that their lack of awareness – is not our main problem.

Unfortunately, we have a much bigger problem.

Our main problem is that we have an inherently insecure system housing immensely valuable data == personal data, intellectual property, business plans and national security information. Unless we understand that our big problem is that we have an inherently weak technical system protecting immensely valuable data-- and begin to address the problem from that perspective --- things are only going to get worse.

Its true most attackers first attempt to enter by finding failures in basic system management. However, if you do all the basics correctly, and you have something worth stealing, attackers will simply escalate to more sophisticated methods to gain entry. In the age of the APT, sophisticated attacks will

successfully compromise any perimeter defense system –even the military's.

In an age when the attack surface is becoming increasingly vulnerable, the attackers are becoming increasingly sophisticated and all the economics favor the attackers it is fool hardy to think that just following basic best practices or assigning personal accountability with heavy penalties will prevent attacks. In fact, the very notion of preventing attacks m—perimeter security – is outdated.

There are only two types of organizations today, those that know they have been successfully compromised, and those that don't know, they have been successfully compromised.

The reality is that is that the cyber attackers are coming after all of us consumers, companies and governments. We are all on the same side in cyber security. The problem is not us its them – the attackers. We must resist the impulse to point fingers at each other and learn how to work together finding 21st century methods to address this 21st century problem.

So, what do we do? (SLIDE 6)

We need to start by realizing we, the good guys, we are all in this together. We are all on the same team and we need to work together collaboratively in a new 21st century model. And we need to go beyond the obsessive focus on the IT departments and the many existing, and often excellent, programs for standard setting and information sharing.

We need to engage our leadership at both the corporate and government levels. We need to have our corporate boards of directors and our most senior government officials evolve a

true understanding of cyber security and how to manage it – we are not going to prevent cyber-attacks any more than we can stop tornados or hurricanes – but we can learn to manage the cyber risk much more effectively.

I am delighted to be able to announce today that these collaborative programs –aimed at our corporate and government leadership --have begun. Moreover, I am happy to announce that the first products resulting from these creative partnerships are now available. They have been independently assessed and judged as successful and they are available to you all, and your peers today, free of change.

Let me now take a few minutes to outline some of these programs and let you know how you can access them.

The first program I'd like to highlight is a collaboration between organizations representing corporate boards of directors and our senior government offices for cyber security. Specifically, the Isa has been working for several years with the National Association of Corporate Directors, elements of their Global network the GDNI and the US Department of Homeland Security and the Germany BSI. These efforts have been directed as creating a series of handbooks for corporate boards of directors to better oversee cyber risk. (SLIDE 7)

These Handbooks, which are now available at no cost on the ISA website (isalliance.org) (SLIDE 8) The AIG website and the BSI website at no charge, are designed first to give the board members a better understanding of the cyber world and the cyber threat. Once that is done we move to what are the steps the board needs to take to successfully fulfil their unique role.

I am proud to say that the program laid out in these handbooks is the only cyber risk management programs I'm aware of that have been independently assessed and found to create actual positive cyber security outcomes.

That is a provocative statement but you don't need to believe me, or BSI or the NACD I'm referring here to the Price Waterhouse in their Global Information Security Survey. (SLIDE 9) Allow me to quote directly from that study:

"The NACD Cyber Risk Handbook recommends that boards view cyber security from an enterprise wide risk management perspective, understand their legal obligations, access sufficient cyber expertise and require management to provide them with frameworks to address the issue including frameworks and a full risk assessment detailing what risks they can accept, mitigate or transfer.

(SLIDE 10) Boards appear to be listening to this advice. Our survey found a substantially increased involvement in board involvement in cyber security leading to on average an increase in budgets in the range of 27 percent.

(SLIDE 11) Other key findings of our survey include that board involvement leads to better risk assessment, closer alignment of cyber security with business goals and the development of a culture of security throughout the organization"

To date we have created 3 editions of these Handbooks, one based on the US model, (SLIDE 12) one adapted for the UK in anticipation of Brexit (SLIDE 13) and of course one done in conjunction with the BSI specifically adapted to the unique structures and perspectives of the German market (SLIDE 14)

Later this year, working with the Organization of American States ISA will be developing an edition for Latin America.

While each of the Handbooks is adapted to the unique needs of the country or culture we are addressing they also follow a coherent set of principles key for boards understanding their unique roles in cyber risk oversight.

Without going into detail, the core principles are: (SLIDE 15)

1. Cyber Security is not an "IT" issue – it is an enterprise wide risk management issue
2. Corporate boards need to educate themselves as to the unique legal and regulatory issues they face with respect to cyber security
3. Boards need to gain access to adequate cyber security expertise
4. Boards need to demand from management that they have developed a comprehensive framework to understand and manage cyber security – both at a technical and structural level
5. Management needs to present boards with a full cyber risk assessment indicating what risks the board needs to accept, what ones they will decline which ones they can mitigate consistent with the boards cyber risk appetite and which risk they can transfer

Some of these Principles are for the board to undertake for themselves. The final two principals have more to do with what the board needs to expect from management.

Principle 1 (SLIDE 16) probably applies equally to both management and the board. We need to understand cyber

security is not an IT issue. In fact, the most common source of a cyber security breach is human, not technical, and so human resource management is just as important for cyber security as is software or hardware management.

Now, for many years IT experts told the boards need to get more involved in cyber security, but what most of these advocates meant was they wanted to teach the boards more about IT. But frankly, the boards don't talk much about ISO standards and NIST Frameworks – and that's probably a good thing. Boards talk about mergers, acquisitions, PE ratios, new product development and strategic partnerships.

So, starting several years ago we took a different approach. Instead of trying to explain IT systems in greater detail to boards, we decided to integrate cyber risk management into their world. In short, instead of demanding that the boards learn our cyber language, we decided to learn their language. So, we asked: What are the cyber security questions the board should ask when considering a merger? Or launching a new product or a new strategic partnership?

Most importantly, we needed to place cyber security risk management in a realistic context. Obviously we need to secure the cyber systems for industry and government. But we need to provide cyber security while also continuing to support our economy, facilitate innovation, provide job growth and protect our citizens. In short, we need to evolve a cyber system that is not just secure but also economically and practically functional in the 21st century.

Aligned with that notion is the fact that the board needs to have determine how much risk they can tolerate we call this their cyber risk appetite – and it can't be zero.

The organization's goal isn't eliminating the cyber threat – the goal is to manage the cyber threat. More specifically, the boards role is not to become IT experts –that's management's role. The board's role is cyber risk oversight

If you have a board, or a CEO or government agency that demands a zero-tolerance policy against cyber-attacks you have a board or CEO that is desperately in need of basic cyber security education.

We will discuss this a bit more in a few minutes.

The second key principle (SLIDE 17) is that boards need to understand the unique legal situation they are in. We don't have time today to go into the varying legal requirements today, but suffice to say that the legal framework for cyber security is quickly evolving and board need to access outside counsel to keep themselves adequately informed.

The third principle (SLIDE 18) for the board is that boards need to access adequate cyber security expertise. It is critical that cyber security not be thought of just in terms of breach management. Cyber security needs to be woven into the business on the front end and part of the entire business development and implementation process. In fact, there is not a single significant business decision in the modern world that doesn't have a significant cyber security component

--- R&D, product development, manufacture, fabrication, strategic partnerships – all business decisions need to be

considered from a cyber perspective –cyber needs to be part of the business.

There is no board that doesn't attempt to have adequate legal expertise on its membership and adequate financial expertise. That makes since because all business decisions have legal and financial aspects. The same is true of cyber security and hence boards need to access that expertise.

Since it's my understanding that at today's conference we have more management representatives than board directors I'd like to focus just a bit more on Principles 4 and 5 as they relate specifically to what management ought to be doing to adequately serve their directors.

Principle 4 argues that management needs to present to their boards a thoughtful structure –both technical and managerial—to address the 21st century cyber problems.

Now most IT departments can readily provide a technical framework for their cyber risk management based on some regulatory or standards model like ISO or NIST. However, most organizations are managerially still structured basically on an industrial age models with segmented departments – legal/finance/human resources/public relations etc -- and little cross-integration.

These segmented models are not necessarily appropriate to the digital age and certainly not for cyber risk management. We propose organizations consider (SLIDE 19) having cyber security managed by a cross-departmental team, operating with a separate dedicated budget –not the IT budget -- which ought to be lead by an executive with cross departmental responsibility like a Chief Operations Officer or even a CEO.

All departments are now cyber departments. Cyber security needs to be understood and engaged across the entire organization and the organization ought to be structured to facilitate that integrated management. Most organizations are not structured this way currently.

The final principle has to do with management providing the board with a full cyber risk assessment. (SLIDE 20) Based on this risk assessment, management needs to provide the board with a clear recommendation as to how much risk they want to undertake, what we referred to a minute ago as the corporate cyber risk appetite.

This calculation includes identifying what data, and how much, the organization is willing to have compromised, how to divide their cyber security investments between basic hygiene and sophisticated defense methods, what options the board may have to transfer some of their risk through insurance and, above all, put in place a cyber risk management plan that they will practice, practice, practice.

Now, to answer these difficult questions well, management needs to move away from the static, traditional model for cyber risk assessment. In fact, as Geer and McClure note in their excellent book, "How to Measure Anything in Cyber Security" its quite possible that the biggest cyber security risk an organization might be taking, may be **the risk assessment method** they are using.

Anyone who has taken a course in statistics is probably familiar with the phrase, "garbage in, garbage out." What this means in a cyber security sense is that if your risk assessment method is overly simplistic, or inadequate it may generate the

wrong conclusions. As a result, you may develop a false sense of confidence in your security methods which might not only waste scarce cyber security resources but could be counter-productive to your security efforts. A sloppy cyber risk assessment method can actually make you LESS secure.

The dominant current cyber risk assessment (SLIDE 21) model is essentially a check list model wherein typically the IT department will go through some list of standards or practices and check off what they have done.

This is not a model that addresses security, it simply addresses compliance – which is an altogether different thing.

The assumption is that the more boxes you check the more mature you are – but that is just an assumption. No one checks all the boxes all the time, so how do you know which un-checked box is important? Many of these systems use color coding or bogus math like rating risks 1-5 but these categories have no real meaning – they are mostly just a guess. This is not systematic risk management.

We need a system for cyber security that looks much more like the systems we use to assess other organizational risks such as financial risk. We need a system that is truly empirical, prioritized and cost based.

As I noted a few minutes ago, over the past few years we have seen a welcome increase in approved spending on cyber security. However, boards are now beginning to face cyber spending exhaustion. They are not going to increase budgets by double digits every year.

Cyber Risk management needs to evolve to a more systematic process (SLIDE 22) that weaves in more than just technical compliance but includes critical thinking, understanding of probability theory, training in calibrated estimation, familiarity with decision models and knowledge of the business context of security decisions.

Fortunately, the market is coming to the rescue. We are now seeing the evolution of a compendium of analytical tools that can be mapped to frameworks like NIST and ISO so that organizations can assess effectives, and cost effectiveness, of their cyber security efforts and thus prioritize their cyber spending. These more modern methods (SLIDE 23) of cyber risk management focus on impacts of attacks, include much clearer definitions which allow for better scoping and less bogus math. These methodologies can place cyber events in quantitative economic terms that allow boards and management to prioritize cyber spending in terms of the business.

Happily, there are a variety of these methodologies that are coming to market. Some are open source like the FAIR or x-analytics model. However they are more complicated than simply check lists so others being offered on a propriety basis by firms like SSIC and even being simplified and blended into insurance products by firms like AIG so that smaller entities can have access to appropriate tools.

Finally these cyber risk handbooks – again available free of charge – include a set of very useful –very brief and easy to use – appendices (SLIDE 24) that help apply these various principles to specific cyber security issues such as what metrics to use, how to address the security of your partners and vendors, how to address the security of your supply chain

and more. They represent the next step in cyber risk management, one that will hopefully help us deal with the ever more sophisticated threats we face in an economically rational way.

However, there is an important note here for government and regulatory agencies. The sort of sophisticated risk management model I have outlined today is not as simple as identifying a checklist of tactics in a generic regulation. To adequately address the ever-evolving cyber threat that is calibrated to specific entities we need to evolve risk management methods that are not generic, but are cost justified based on the unique business and cultural parameters. Requiring entities to comply with prescriptions that are not empirically shown to be effective and cost effective can actually be harmful to our overall security posture.

So just as industry needs to evolve to face the increasing cyber threat so too must government. The traditional model wherein government takes on a somewhat paternal role – disciplining its unruly and selfish industry children to protect the consumer needs to evolve. As I have said, in the cyber security world we are all on the same team. We would suggest the need to evolve a model that looks more like a successful marriage – where government and industry are co-equal partners in securing the common networks we share.

At ISA we have actually spelled out the principles of this evolved partnership model by adapting the historic European philosophies known as the Social Contract and have proposed a Cyber Security Social Contract. (SLIDE 25) – but that discussion would require another keynote at another time.

Let me conclude by noting one of the unique things about the digital age is that it came upon us all so quickly so completely and so easily that we really didn't have time to think through the implications of such broad use of digital systems. I don't think it's too late.

I think if we truly pull together we can help develop a sustainable approach to cyber risk management. Someone once said some are born great, others strive to achieve greatness and still others have greatness thrust upon them. I think those of us in the cyber security field have had that opportunity for greatness thrust upon us. Let's live up to that challenge together

Thank you.