Science AMA Series: Hello, I'm Joe Scherrer. I was an IT and cybersecurity innovator with the U.S. Air Force, and now am director of the cybersecurity initiative at Washington University in St. Louis. AMA!

Joe$_{S}$*cherrer*[1]*andr*/*ScienceAMAs*[1]

[1]Affiliation not available

April 17, 2023

Abstract

Hello, I'm Joe Scherrer. I spent the first part of my career as an information technology and cybersecurity innovator with the U.S. Air Force, culminating as the commander of the Air Force's only combat-coded deployable communications wing. Now, I am director of the cybersecurity initiative and program director of graduate studies in information systems management and cybersecurity management at Washington University in St. Louis, where I help to train future leaders in cybersecurity who can deal with the constant threat of security breaches by large organizations. I'll be back at 3 pm ET to answer your questions, AMA! Edit: Thanks for all of the great questions. I enjoyed this!

the WINNOWER

REDDIT

Science AMA Series: Hello, I'm Joe Scherrer. I was an IT and cybersecurity innovator with the U.S. Air Force, and now am director of the cybersecurity initiative at Washington University in St. Louis. AMA!

JOE_SCHERRER R/SCIENCE

Hello, I'm Joe Scherrer. I spent the first part of my career as an information technology and cybersecurity innovator with the U.S. Air Force, culminating as the commander of the Air Force's only combat-coded deployable communications wing. Now, I am director of the cybersecurity initiative and program director of graduate studies in information systems management and cybersecurity management at Washington University in St. Louis, where I help to train future leaders in cybersecurity who can deal with the constant threat of security breaches by large organizations.
I'll be back at 3 pm ET to answer your questions, AMA!
Edit: Thanks for all of the great questions. I enjoyed this!

CORRESPONDENCE:

DATE RECEIVED:
November 08, 2017

DOI:
10.15200/winn.151005.55476

ARCHIVED:
November 07, 2017

CITATION:
Joe_Scherrer , r/Science , Science AMA Series: Hello, I'm Joe Scherrer. I was an IT and cybersecurity innovator with the U.S. Air Force, and now am director of the cybersecurity initiative at Washington University in St. Louis. AMA!, *The Winnower* 4:e151005.55476 , 2017 , DOI: 10.15200/winn.151005.55476

What subjects would you recommend for computer scientists with a more cursory interest in cybersecurity?

jatatcdc

What subjects would you recommend for computer scientists with a more cursory interest in cybersecurity? We've researched this very question fairly thoroughly here at Washington University as part of our efforts to roll out a Masters in Cybersecurity Engineering degree in Fall 2018. For someone like you who has a technical background in computer science or computer engineering and who wants to add skills/knowledge in a deep and meaningful way, here's what I recommend: Network Security Secure Operating Systems Security of the Internet of Things Systems Security from the Perspective of a Malicious Actor Secure Software Engineering The above subject areas, especially if done from a rigorous STEM-based perspective will be excellent enhancements to your CS repertoire.

What's your take on cryptocurrency security?

-lestat-

Well, cryptocurrency is here to stay in its many different incarnations. When we're talking about cryptocurrency security, we're mainly talking about blockchain which uses cryptographic techniques to ensure the validity of the transaction record. That said, cryptocurrencies are not immune to hacking. Case in point, Bitcoin has seen over 40 hacks of various kinds since its inception. Anywhere there is money or perceived value to be had, criminals will devise ways to get at it. So, if cryptocurrency is here to say so is the hacking and theft of cryptocurrency. The Cryptocurrency Certification Consortium has

promulgated a set of standards (CryptoCurrency Security Standard (CCSS)) that specifies various levels of requirements to secure IT systems upon which cryptocurrency algorithms run. So, the "industry" has recognized what I think will be a growing threat and has moved to deal it. I think this is just the first set of shots that have been fired in a much bigger war, however.

Read more: Cryptocurrency Definition | Investopedia https://www.investopedia.com/terms/c/cryptocurrency.asp#ixzz4xmVnfvvw Follow us: Investopedia on Facebook

1. What are your worst fears within cybercrime and cybersecurity.
2. We have all seen what custom malware like struxnet can do - What do you imagen we will see in the future?
3. The new European data retention police (GDPR) will take effect next year (may 25). It focuses on punishing organizations that doesnt account for IT security or take it serious for that matter. Do you think this is the right way about IT Security and awareness. Why / why not?

Doublewobble

1. Cybercrime: the proliferation of "nation-state grade" cyber weapons to dark net criminal actors and the ever-increasing sophistication of those weapons with the will to use them. Cybersecurity: Three letters: IoT. The Internet of Things. If we think achieving security of billions of interconnected devices, systems, and connections is hard today, wait until that number goes up to trillions or more. Plus, very, very few organizations are thinking about IoT security in any meaningful way.
2. As alluded to above, Stuxnet is just the tip of the iceberg and we're (modern society) the Titanic. I don't worry as much about nation-states per se as I do extra-territorial criminal cartels using their capabilities to destroy companies, act as proxies for nation-states, etc.
3. For various reasons, the EU has adopted a much more putative stance. Ultimately, if you want to "incentivize" bad behavior, you have to impose some sort of costs. The EU has chosen to hit organizations in the wallet. It would be interesting to see what would happen (if you could ensure no corruption), if an organization were REWARDED for excellent cybersecurity practices.

Hi and thanks for joining us today!

Can you explain why blockchain might be superior to HL7 and if agencies like HHS and CDC should begin implementing it?

PHealthy

Thanks PHealthy. I'd love to answer your question, but besides blockchain this one is beyond my expertise since I do not work in the healthcare field.

Hi there! I was wondering something about your work. What's exactly the task of a deployable programming unit? What would you do in a combat environment? Do cyber security experts in the army need to have the same physical capabilities as "active" people?

lucaxx85

The communications part of the mission involved setting up a secure communications (phones, radios, etc.) and IT infrastructure in a "bare-base" deployed situation for squadron-sized (6-8 jets) units all the way up to wing-sized units (2000-3000 people, multiple squadrons of jets, support activities like logistics, medical, engineering, etc). The combat part of the mission meant we had to do the above in

"contested" environments while under fire from opposing forces. In answer to your question about physical capabilities: yes, all Airmen, sailors, soldiers, and Marines must meet a minimum set of physical standards no matter their career field. War is tough business, you must be able to withstand the mental and physical stresses involved.

It seems to me, an end-user, that *basic* security rules in an organization are simply impossible to impose. E.g: No shared accounts, no passwords written on the keyboard etc...etc...

I work in a hospital and the IT security team is basically crying every single day. Yet, many of the simplest things they require us users (e.g.: no shared accounts) are technically impossible to implement in many cases. (E.g.: the authentication procedure required to operate a sensitive machine is incompatible with the site-wide authentication procedures).

How do you deal with these things?

lucaxx85

Well, I'm a big believer in "blocking and tackling" when it comes to cybersecurity. The vast majority of security incidents would simply go away if everyone in the organization practiced good cyber hygiene. In your particular situation, it seems like the security controls that are in place have not been evaluated in terms of 1) technical feasibility, 2) operational impact, and 3) effectiveness. Strong security means more than checking off a top 10 list of "best practices." What I would do in your case is document how the IT security team's requirements are impacting your ability to do your job and send that to the CIO or CISO (run it pass your boss first). As I tell our students, cybersecurity is all about recognizing, assessing, and mitigating risk in terms of the BUSINESS or OPERATIONAL requirements of the organization. There are a lot of things a savvy cybersecurity practitioner can do in addition to imposing technical controls. That's the discussion you want to get to.

How much of your work focusses on technical faults and how much on the human factors in cyber security?

thijser2

Our approach at Washington University is based on the reality that there are bad actors in the world who use technology for nefarious ends. In other words, it's not solely about the technology, but rather the total environment in which humans use that technology. Focusing an organization's effort solely on "technical faults" is a mistake. Equal--if not more--attention should be given to strategy, governance, policy, security controls, active and engaged management, and training. So we take a comprehensive socio-technical approach to cybersecurity.

What was the worst breach you'd had to deal with, if there was one?

useful_person

I was stationed at the Pentagon from 2005-2007, the height of the Iraq war, not to mention U.S. operations in Afghanistan. My chain of command was President Bush, Chairman of the Joint Chiefs of Staff General Peter Pace, and Director of Communications Systems, Lieutentant General Bob Shea, then me. I received word that Secretary of Defense Rumsfeld and many other senior civilians, generals, and admirals had the unclassified email accounts breached. That was the first indication that a large Asian country had broken into our networks. Fast forward a month or so and I was assigned to lead a team to write the U.S. Department of Defense's first National Military Strategy for cyberspace

operations. That was as the strategic level. A whole host of tactical efforts were undertaken to deal with this breach.

In the UK, the WannaCry ramsomware virus earlier this year had a massive impact on the national health system, paralyzing several hospitals, which caused a direct impact on human lives. The virus took advantage of a windows vulnerability discovered by the NSA, that chose not to disclose it. A leak of this information then allowed hackers to use it to create said virus. What's your opinion on this kind of practices by government agencies? Also, despite all the recent attacks, cybersecurity is still not a major concern for most companies, governments, etc, with the IT departments continuing to be underfunded and understaffed to deal with these problems. What do you think should be done to deal with this situation?

MadScience98

In my part of the world, I'm seeing the light bulb come on for companies, government, etc. when it comes to cybersecurity, especially when compared to even 5 years ago. No one wants to end up on the front page of the New York Times or the evening news. That said, cyber criminals have figured out that small to medium sized organizations are juicy targets and very lucrative for them. In these orgs, there might be an IT staff (or not) and very little to no focus on security. It's like leaving your unlocked car running in a parking lot--easy pickings. So, there is a lot of work to be done, especially from an education and awareness standpoint. With regard to the NSA, and we should add other top tier nation-state signals intelligence agencies, their job is to eavesdrop on other countries. They are spy agencies. So, we'll never get away from this kind of secretive and parochial behavior. What we ought to expect, at least from countries that respect the rule of law is that an internal, risk-based vetting process take place when deciding to disclose or not disclose.

Do you believe the RMF is a sustainable process or should we expect a more streamlined process to roll out in the next decade?

StronglyIrregular

My $.02. RMF is better that what the U.S. Department of Defense has now which is overly bureaucratic, cumbersome, and slow. Of course, the RMF is itself a bureaucratic process, but one that looks to be thoughtfully designed. That said, you can be sure that the process will be refined once it hits the turbulence of actually being performed in living-breathing organizations.

Is a complete abandoning of conventional money a real possibilty with the rise of Cryptocurrencies? When can human society expect such a move?

redzimunze

Short answer: not unless nation-state central banks can assure themselves that they can control such currency...which will be very difficult.

Is the whole mess around Intel ME and other "ring -1", "ring -2" stuff at all relevant today (for me as a private user | for a high profile target), or is it just a drop in an ocean of OS, application and social engineering vulnerabilities?

Jonas_O

Hierarchical protection rings constitute an interesting approach to operating system security and something we would cover in our operating systems and advanced operating systems courses. The Multics OS was the most robust implementation of this approach using all 8 rings, but has fallen into disuse. I think some manner of a "ring" architecture ought to be considered in the design of both chipsets and OSs...the devil, however, is in the details and in the implementation (and the potential for market share and sales). Even so, as you say, there are many other vulnerabilities and mitigation techniques that need to be considered in OS design. If you enroll in our degree program, you'll be able to learn much more about all this. :>)

what do you think is the realistic vs needed budget difference for cyber security in the whole country? Also what is the level of protection we are at on average against the never sleep hackers movement? ... aside from regular people, ...many banks an organizations get hacked and we never hear about them...

Gallionella

A good rule of thumb for the portion of your IT budget that should be allocated to cybersecurity is 10%-20%. Of course, more would be better (to a point). In reality, cybersecurity spend must be evaluated in terms of business risk. Agree that many organizations get hacked and it's not publicized. Even so, the cost of mitigating those breaches need to come somewhere which means resources must be shifted and the cost of doing business goes up.

What are the latest developments when it comes to post-quantum cryptography?

How big of a concern is it at the moment from a cybersecurity point of view?

Would current solutions impact the ease of use of secure web services as we know them today?

Thanks!

c_rap

I get this question a lot in my cryptography course where we spend a bit of time on quantum computing and its impact on symmetric and asymmetric cryptography. First, quantum computing has not yet matured and proliferating as a viable technology. Depending on which expert you talk to, we're anywhere from 10-20 years or 100 years or more before we're at a point that quantum computing will decisively undermine the world's current cryptographic algorithms. In my view, we're a long way away from a "crisis" in this regard because the current symmetric algorithms have plenty of legs to deal with what is a non-existential threat. As far as post-quantum cryptography research goes there is a very active global cadre of researchers who are laying the groundwork for the next generation of cryptographic algorithms. Fruitful areas of exploration include: lattice-based cryptography, multivariate cryptography, hash-based cryptography, code-based cryptography, supersingular elliptic curve isogeny cryptography, symmetric key quantum resistance. The folks working in these areas are wicked-smart and I look forward to hearing of actual real-world testing and implementation of such algorithms.

Hi Joe. What are some common, easily-addressable security gaps you often see in large organizations?

RogueJD

- Lack of an employee cybersecurity training and awareness program. Very good bang for the buck and an absolutely essential part of a robust cybersecurity approach.
- Default or easily cracked passwords on end-user devices and/or IT systems and network machines.
- No vulnerability patching process (e.g. anti-virus)
- Improper cryptographic key management (including "stale" keys that haven't been changed in a while)
- Not keeping your owner, president, partner, etc. up-to-speed on cybersecurity status and challenges
- Not having a business continuity plan (and exercising that plan) in the event of a breach

Are you aware of the phenomena of teens and young adults engaging in behavior they intend to create social upheaval not because they are trying to affect change but simply because they think the resulting chaos is funny? I ask because I've heard several 16-25 year olds express this sentiment, particularly in reference to the chaos created by the bizzare fake news during the last election cycle. Ever since I've been saying someone really needs to explain 4chan to the government because it's definitely more than jokes going on.

drgk23

Several random thoughts here: Organizationally, I don't see this as much of a cybersecurity issue as an employee code of conduct issue. From the standpoint of a civil society, in the U.S. we have the rights of freedom of speech and freedom of assembly so this type of part of our system. Fake news is not outlawed (if it were we wouldn't have supermarket tabloids). When it comes to the revolutionary overflow of the U.S. government, however, we're in different territory and the U.S. criminal code applies. Ideologically, the type of behavior you allude to aligns with various U.S. anarchic and communist movements. As a practical matter, for the most part we're talking about youthful folly, mostly uninformed. It's up to each of us as citizens to select our news sources and the way we form our opinions. Unfortunately, far too many are tossed around on the volatile winds of hearsay and opinion.

I am a CCNP with only high school diploma...would you please recommend me IT courses so i can start a career in security..due to family problems and remote location i cannot at all aford to go to college so that is out of option. Thanks in advance

ncrixz

I'd recommend searching the Internet for a technical college that offers online degrees in cybersecurity, then taking a look at the course listings to get an idea of what they offer. For someone like you who is thinking about a career in cybersecurity, a credible degree would be very helpful. I'd also look at getting certifications such as CISSP.

what is the best way of dealing with a computer virus

zweetandzour123

Can you give me a little more information? Is this something you individually are experiencing now? Or are you talking about a general problem in an organization?