# Women Reshaping The Cybersecurity Industry: Dr Sarbari Gupta Of Electrosoft Services On The Five Things You Need To Create A Highly Successful Career In The Cybersecurity Industry

An Interview With David Leichner

Get educated — Learn the basics of computers and networking through formal coursework or self-learning.

*The cybersecurity industry has become so essential and exciting. What is coming around the corner? What are the concerns we should keep an eye out for? How does one succeed in the cybersecurity industry? As a part of this interview series we had the pleasure of interviewing Dr. Sarbari Gupta.*

*Dr. Sarbari Gupta has been active in the information security industry for over 20 years, specializing in cybersecurity, digital identity and access management, and cloud security. She holds PhD, MS and BTech degrees in Electrical Engineering as well as CISSP and CISA certifications. Dr. Gupta, a frequent speaker at industry conferences on cybersecurity topics, has authored over 40 technical papers/presentations on leading-edge topics and holds four patents in areas of cryptography. She has co-authored several NIST Special Publications in the areas of Electronic Authentication (SP 800–63), Security Configuration Management (SP 800–128), and Mobile Credentials (SP 800–157). She is the recipient of many accolades including Distinguished Alumnus Award from Indian Institute of Technology (Kharagpur); NOVA/PSC GovCon Executive of the Year (under $75M); FedHealthIT Women in Leadership Impact Award; U.S. Women's Chamber of Commerce's Stellar Award; Silver*

*Stevie® Award for Female Executive of the Year; and the Washington Business Journal Minority Business Leader Award.*

**Thank you so much for doing this with us! Before we dig in, our readers would like to get to know you a bit. Can you tell us a bit about your backstory and how you grew up?**

I grew up in Kolkata, India. My father was an engineer and my mother a homemaker. I am the middle child of three siblings. While I lived with my family in Kolkata through most of my early years, our family did reside near Chicago for a few years while my father was doing an MBA at Roosevelt University. Since I always loved math and science, I opted to attend an engineering college. After completing my undergraduate engineering degree at the Indian Institute of Technology, Kharagpur, India, I came to the United States to pursue a graduate education in Electrical Engineering. During that time, I discovered the novel new area of computer and data security; I have been focused on the cybersecurity arena ever since. After graduate school at the University of Maryland, College Park, I worked for several companies based in the Washington, DC area until I got the entrepreneurial itch in 2001 and launched Electrosoft as a government contracting company specializing in cybersecurity.

**Is there a particular book, film, or podcast that made a significant impact on you? Can you share a story or explain why it resonated with you so much?**

Yes, an audio program that I came across many years ago had a major impact on my mindset and strategies for life. It was "Lead the Field" by Earl Nightingale. It offers twelve major principles for self-development for becoming a leader in any field. Several of these principles really resonated with me: "The Magic Word (Attitude)," "A Worthy Destination (Setting Goals)," "The Miracle of Your Mind," "Seed for Achievement (Integrity)" and "Living One Day at a Time."

In listening to these messages over and over again across the years, I understood that I am in charge of my life and can create my world rather than react to circumstances. This feeling of empowerment has had an immense impact on my life trajectory!

**Is there a particular story that inspired you to pursue a career in cybersecurity? We'd love to hear it.**

In graduate school, my focus was computer engineering. Some of the operating systems courses I took were taught by Dr. Virgil Gligor, a leading expert in operating system security and cryptography. I was intrigued by the concepts he taught (including many of the core tenets from the Department of Defense Orange Book) and felt drawn to pursue this emerging field as my focus for further study and research. I started working under Dr. Gligor for my doctoral thesis, which focused on models and artificial intelligence–based techniques to identify patterns of vulnerabilities in operating system source code and developing principles for mitigating such vulnerabilities to make the operating system resistant to compromise. At the same time, the World Wide Web was taking shape and protecting data and computers from internet hackers became relevant to every organization and later every individual. After finishing graduate school, I started working for a high-end cybersecurity research and development firm. I have never looked back since. The field of cybersecurity has become more critical and interesting through the years!

**Are you working on any exciting new projects now? How do you think that will help people?**

Yes, several new projects are very interesting and exciting!

My team and I are looking at technologies (such as the Open Security Control Assessment Language or OSCAL) and tools that make it possible to reduce the manual workload for documenting and reviewing security controls implemented by government information systems to determine compliance with the Federal Information Security Modernization Act and Federal Risk and Authorization Management Program. We are working with several federal customers to introduce such technologies and tools into their current environment so that the implementation of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and achievement of Authorization to Operate (ATO) and Continuous ATO can be achieved with less manual effort, less time and fewer errors than current processes. This project excites me as it is a channel for innovation that can dramatically improve the security posture of government information systems while reducing costs and time.

Another area that we are looking at is the use of passwordless authentication techniques (such as FIDO2 or passkeys) within the federal government environment. Passkeys leverage asymmetric cryptographic keys activated with a second factor such as a PIN or a biometric. This technology was developed jointly under the FIDO Alliance by some of the leading technology behemoths like Microsoft, Google, Apple and others. As of mid-2022, passkey technology is available and supported on most major operating systems and browsers including mobile environments. At Electrosoft, we are working with our federal customers to define ways to utilize passkey technology by government staff who are currently required to use smart cards to authenticate themselves to government networks and systems. These techniques could offer a dramatic boost to the security of government systems while also improving the usability and robustness of authentication solutions available to the end users.

**Ok super. Thank you for all that. Let's now shift to the main focus of our interview. The Cybersecurity industry seems so exciting right now. What are the 3 things in particular that most excite you about the industry? Can you explain or give an example?**

Three things that excite me include:

1. Passwordless Authentication Solutions that use strong cryptography (as described above) while offering user-friendly interfaces on a broad set of platforms.

2. Use of Artificial Intelligence (AI) and Machine Learning (ML) technologies to improve the capability of applications and solutions to progressively improve their effectiveness in automatically identifying and eradicating cyber threats in IT environments without engaging with the end user.

3. The heightened interest in implementing the holistic cybersecurity strategy known as Zero Trust. Recent regulatory initiatives make it mandatory for federal civilian and defense agencies to pursue a comprehensive set of actions to plan for and implement a Zero Trust Architecture (ZTA) within their environments. This focus on Zero Trust has resulted in a flurry of creativity within the cybersecurity technology sector, leading to new products and services that help organizations roll out various elements of a ZTA.

**What are the 3 things that concern you about the Cybersecurity industry? Can you explain? What can be done to address those concerns?**

Three things that concern me include:

1. End users remain the weakest link in the cybersecurity chain and can easily fall prey to malware and ransomware attacks despite their organization's best efforts to protect the environment through technologies and tools. End-user training helps address this problem, however, certain malware and phishing attacks remain difficult to spot and avoid.

2. The maturity of cybersecurity programs in many organizations within critical infrastructure sectors (energy, food supply, healthcare, transportation, etc.) is low, and these sectors are imminently vulnerable to attacks from a motivated and knowledgeable adversary. Moreover, many of the operational technology (OT) systems used with these organizations are susceptible to the same types of cybersecurity attacks as the IT environment, however, most OT systems are not capable of being fortified against such attacks. This disparity creates a huge risk to the nation and every citizen.

3. The complexity of the cybersecurity arena increases every day as hackers and bad actors find newer and more novel ways to penetrate and compromise organizational systems and data. We lack enough people, processes, technologies, money and time to secure our current systems. Ultimately, it is a risk management game where organizations need to prioritize their cybersecurity efforts based on risk to the organization and what their budget can accommodate.

**Can you share how you are helping to reshape the cybersecurity industry?**

At Electrosoft, we are privileged to work with NIST to support the development of cybersecurity standards and specifications in the area of identity management, authentication and cyber risk management. The publications we help to develop in support of NIST guide the implementation of effective cybersecurity programs and systems. Federal government organizations must use these NIST publications; many other organizations, both national and international, voluntarily leverage them.

We also serve the General Services Administration (GSA) and provide policy and governance support for the Federal Public Key Infrastructure (FPKI), which provides the trust fabric for authentication and secure transactions within the federal IT ecosystem. The FPKI provides trust for every PIV (Personal Identity Verification) card and every CAC (Common Access Card) that federal staff use to authenticate to their agency systems and networks or to sign/encrypt online communications and transactions. The FPKI also provides the trust fabric for interactions between federal government systems.

As mentioned before, we are working to introduce increased automation in the government's ability to authorize systems from a cybersecurity perspective. We expect this transition to significantly improve the security posture of federal government information systems at lower cost and effort.

Finally, our efforts to introduce strong, passwordless authentication technologies and tools into federal government environments will dramatically reduce the effectiveness of phishing attacks on vulnerable users working within such environments.

**As products, devices and vehicles become connected, this is creating a new and emerging threat vector. How do you think manufacturers and their customers should prepare to be as safe as they can be?**

Supply chain security and secure coding practices are essential elements that manufacturers of IT, OT and Internet of Things (IoT) systems have to embrace to improve the safety and reliability of the products and services they offer end customers.

**Can you share a story from your experience about a cybersecurity breach that you helped fix or stop? What were the main takeaways from that story?**

Electrosoft has teams of cybersecurity engineers and analysts operating Security Operations Centers (SOCs) for our federal agency customers. Our SOC engineers and analysts work 24x7x365 monitoring networks and activities to identify possible intrusions, investigate potential threats and take rapid action to neutralize or stop actual attacks. In April 2023 alone, our SOC team at a civilian agency stopped 6,151 pieces of malware, quarantined 1,549 emails with personally identifiable information (PII) and conducted more than a dozen investigations of possible intrusions. The main takeaway is that cyber threats are constant and evolving. That's why Electrosoft assures our cyber analysts keep current with the latest tools as well as the Tactics, Techniques, and Procedures (TTPs) used by threat actors.

**As you know, breaches or hacks can occur even for those who are best prepared, and no one will be aware of it for a while. Are there 3 or 4 signs that a layperson can see or look for that might indicate that something might be amiss?**

For the layperson at home, it is vital to be able to spot phishing attempts via email or other messaging channels. If a message seems to create a sense of urgency or panic, requests sensitive information (such as a password or PII) or prompts immediate opening of an attachment or clicking on a link, it is important to take a breath and consider the possibility of a phishing scheme. At home, it is best to delete the message immediately if its legitimacy cannot be confirmed. At work, one should report the message to the IT department.

Beware of a website or application that presents an offer that seems too good to be true. It is probably prompting you to download content to your local machine that contains malware that can steal your sensitive information or do other types of harm to systems on your network.

If your computer starts to behave differently or is slower after downloading or installing new software, it is possible that the computer is infected with malware. Consult with your IT department at work (if this is a work computer) or run your anti-virus or endpoint detection tool (which you should have on every computer) to scan your computer for malware.

**After a company is made aware of a data or security breach, what are the most important things they should do to protect themselves further, as well as protect their customers?**

1. Isolate the system or network segment that was breached as soon as possible to prevent the breach from spreading throughout the rest of the network.

2. Gather evidence related to the attack such as details of the systems that were compromised, forensic images of the breached systems, audit logs from the affected or related systems, type and timing of the possible event(s) that led to the breach, etc. Document and preserve the evidence.

3. Perform technical analysis of the evidence to identify unusual activities and indicators of compromise, correlate events, analyze for use of common TTPs to determine the probable methodology and define the scope of the breach.

4. Eradicate the source of the breach based on previous analyses, restore the affected systems and address the identified vulnerabilities that led to the breach.

5. Test the reinstated systems to ensure that the breach has been corrected and ensure that the systems are safe to use by stakeholders and customers.

There are many excellent resources available on the internet at no cost. NIST and CISA (Cybersecurity and Infrastructure Security Agency) offer several valuable resources to assist organizations with cyber incident detection and response including NIST Special Publication 800–61, Rev 2: Computer Security Incident Handling Guide and CISA's Cybersecurity Incident & Vulnerability Response Playbooks.

**What are the most common data security and cybersecurity mistakes you have seen companies make? What are the essential steps that companies should take to avoid or correct those errors?**

Some of the most common cybersecurity mistakes I have observed include:

1. Not implementing and enforcing multifactor authentication for the organization's staff.

2. Putting sensitive information (such as Social Security numbers, salary data, etc.) in unencrypted files on their network or SharePoint.

3. Not limiting access to various resources on their network based on least privilege and need to know.

4. Not running regular vulnerability scans on their network and endpoints.

5. Not maintaining regular backups of all important organizational data and files and not regularly testing to ensure that backups can be leveraged to restore files.

**Thank you for all of this. Here is the main question of our discussion. What are your "Five Things You Need To Create A Highly Successful Career In The Cybersecurity Industry?**

1 . Get educated — Learn the basics of computers and networking through formal coursework or self-learning.

2 . Get Certified — Obtain general cybersecurity certifications such as Sec+, CISSP or cybersecurity tool certifications to have the credibility to apply for cybersecurity positions. Participate in bootcamp courses to speed up progress.

3 . Get Hands-on Experience — Set up an IT environment where you can dabble and experiment with different cyberattack techniques and free or low-cost tools in a safe and self-contained environment.

4 . Get a Cybersecurity Role or Job — Seek or volunteer for cybersecurity-related tasks or roles in your existing job to obtain experience. Find and apply for a cybersecurity-focused job or position.

5 . Stay Connected — Maintain and increase your knowledge of the field through self-study, continuing education, embracing opportunities to participate in various cybersecurity projects and thought leadership activities to keep pace with the rapidly evolving space of cybersecurity. Create your own “brand” as a cybersecurity expert.

**We are very blessed that very prominent leaders read this column. Is there a person in the world, or in the US with whom you would like to have a private breakfast or lunch, and why? He or she might just see this if we tag them :-)**

If the opportunity presented itself, I would love to have a chat with Chris DeRusha, the Federal Chief Information Security Officer, Office of Management and Budget. I would like to hear his thoughts on the most critical areas of focus to raise the cybersecurity posture of the entire nation and his opinions on ways to enable zero trust implementation, secure the software supply chain and protect digital assets in the post quantum world.

**Thank you so much for these excellent stories and insights. We wish you continued success in your great work!**