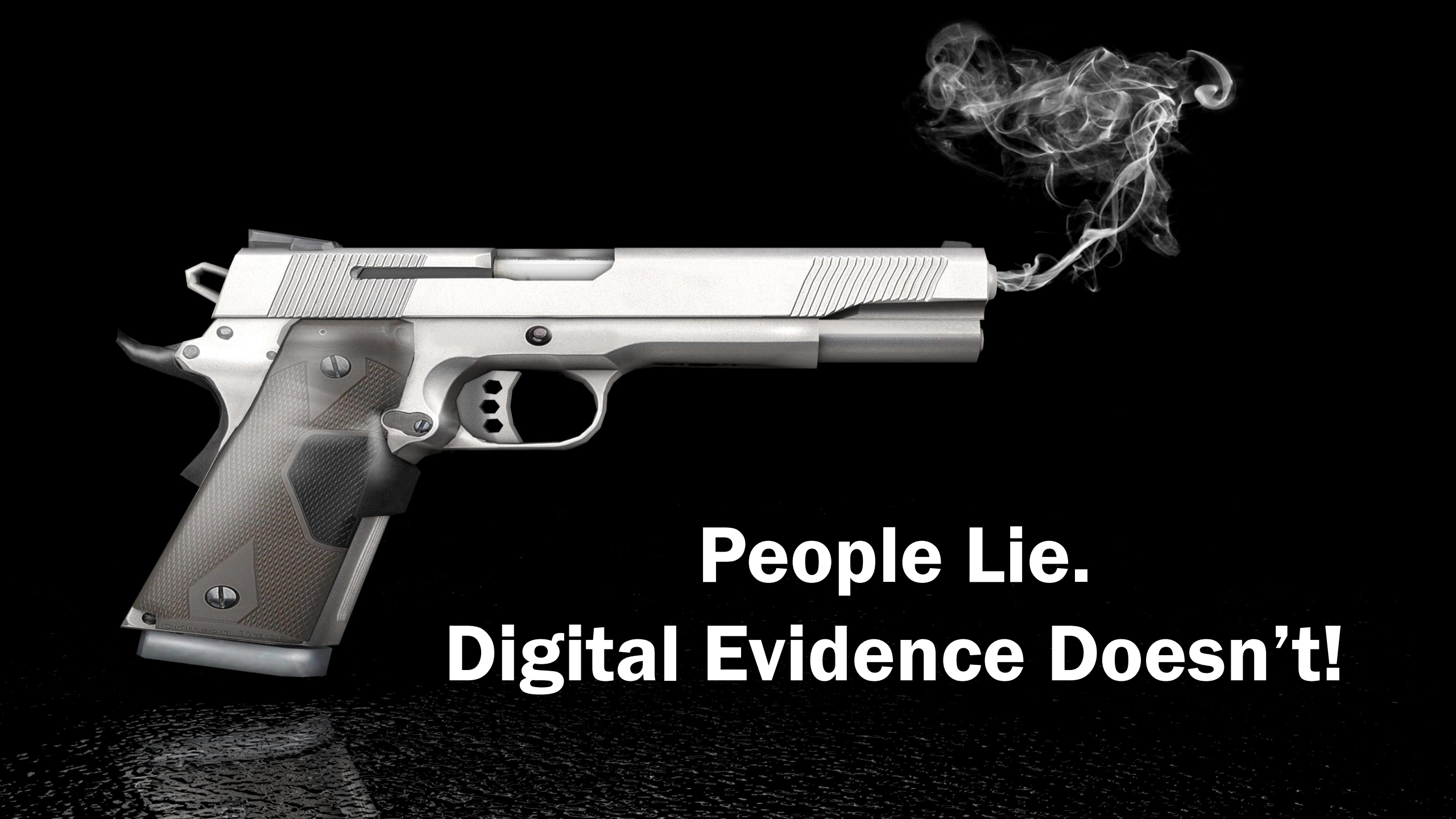

People Lie.
Digital Evidence Doesn't!

Digital Litigation Support Services

Digital litigation support relies on the accurate identification, collection, preservation, and interpretation of electronic data submitted as evidence for legal matters in a court of law.

Digital4nx GROUP

...Bridging the Legal and Technology Gap

Areas of Practice

- ❑ Digital Forensic Investigations and Expert Testimony
- ❑ Electronic Discovery Hosting, Consulting, and Advisory
- ❑ Early Case Assessment - ECA

Civil and Criminal	Common Types of Matters	Plaintiff or Defense
✓ Employment	✓ Commercial Litigation	✓ Criminal Defense
✓ Restricted Covenant & Non-Compete, ✓ Harassment, Discrimination	✓ Partnership Divorce ✓ Breach of Contract ✓ Fraud ✓ Internal Investigations – Subpoena Requests	✓ Embezzlement ✓ Fraudulent Misconduct ✓ Compliance Violations
✓ Data Theft & Theft of IP	✓ Matrimonial ✓ Personal Injury	✓ Other

Digital4nx GROUP

...Bridging the Legal and Technology Gap

Steps for conducting a Digital Forensic Investigation

Uncovering Information Using Digital Forensics:

How did it happen, who is affected, and what are the risks. Timely forensic analysis can help you contain the damage and determine the scope of the breach.

Step 1 : Collection / Extraction

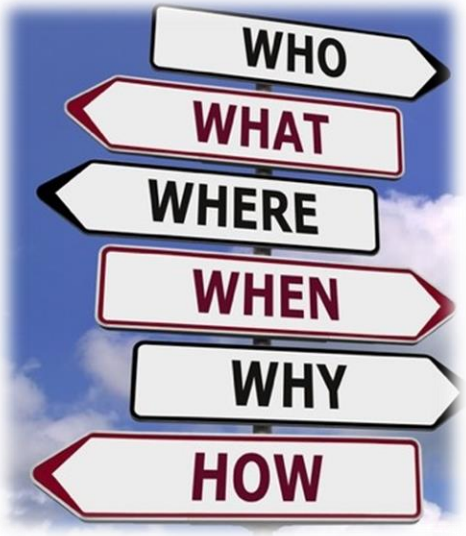
Step 2 : Identification

Step 3 : Analysis

- Recover and search deleted files, formatted drives, email, and other data thought to be erased
- Examine file related metadata
- File creation, modification, deletion, and last accessed dates
- User ID used to create modify and access data
- Operating system artifacts
- When and to what printer a file was printed
- If a web site was accessed via a link or typed in
- If a drive or USB was connected and what type

Step 4 : Documentation

Step 5 : Testimony (Written, Oral, Video)



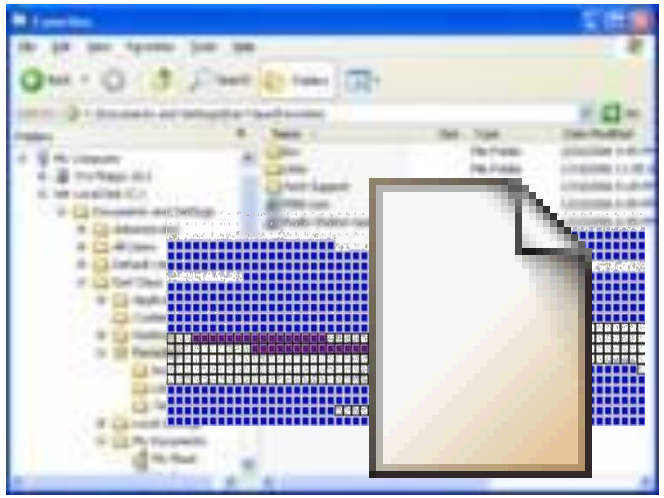
Digital4nx GROUP

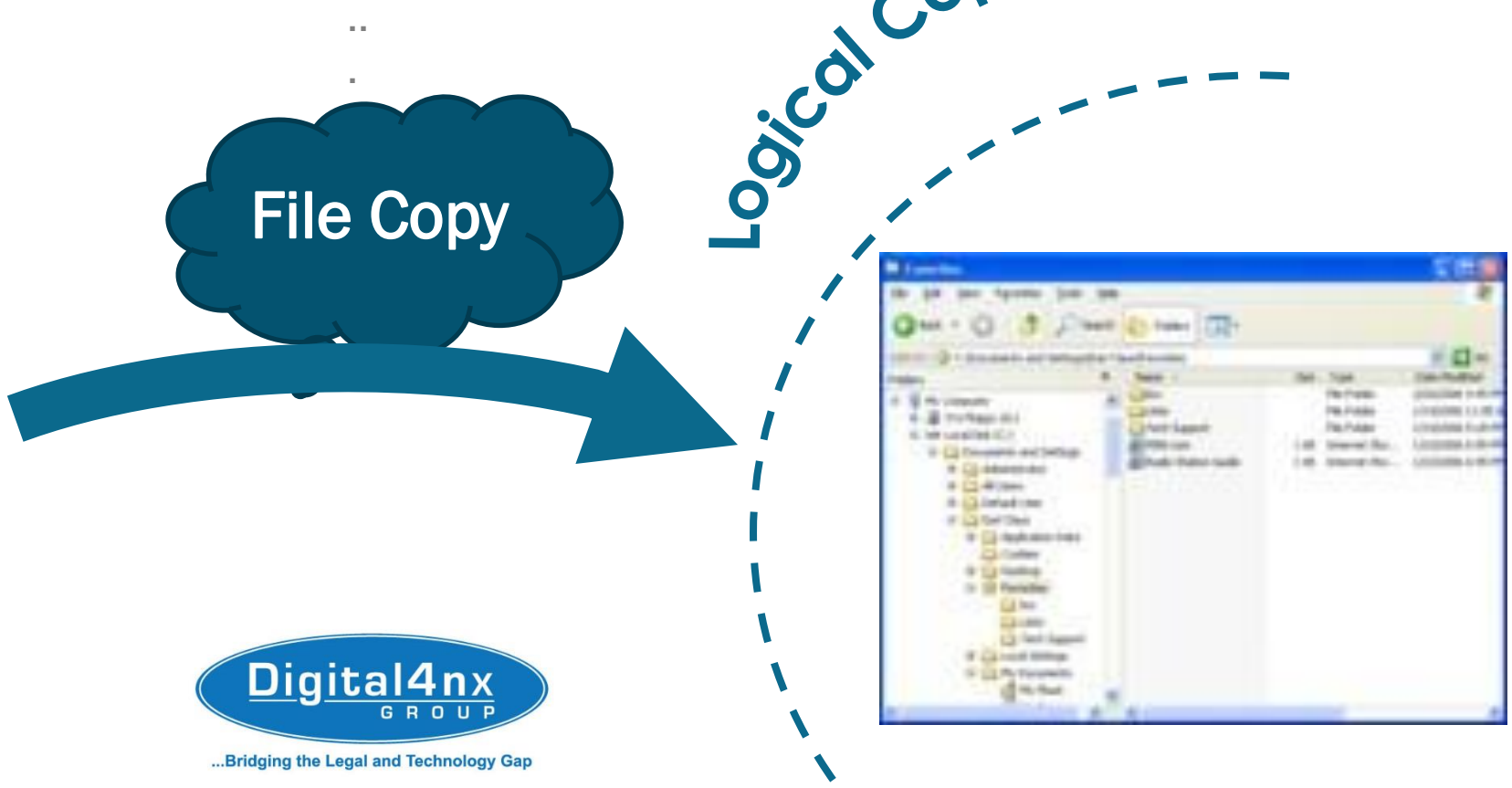
...Bridging the Legal and Technology Gap

Preservation: Copying Logical Files

- Copying files from one folder to another.
- Original evidence **is** changed.
- Hidden data is **not** copied.

Original



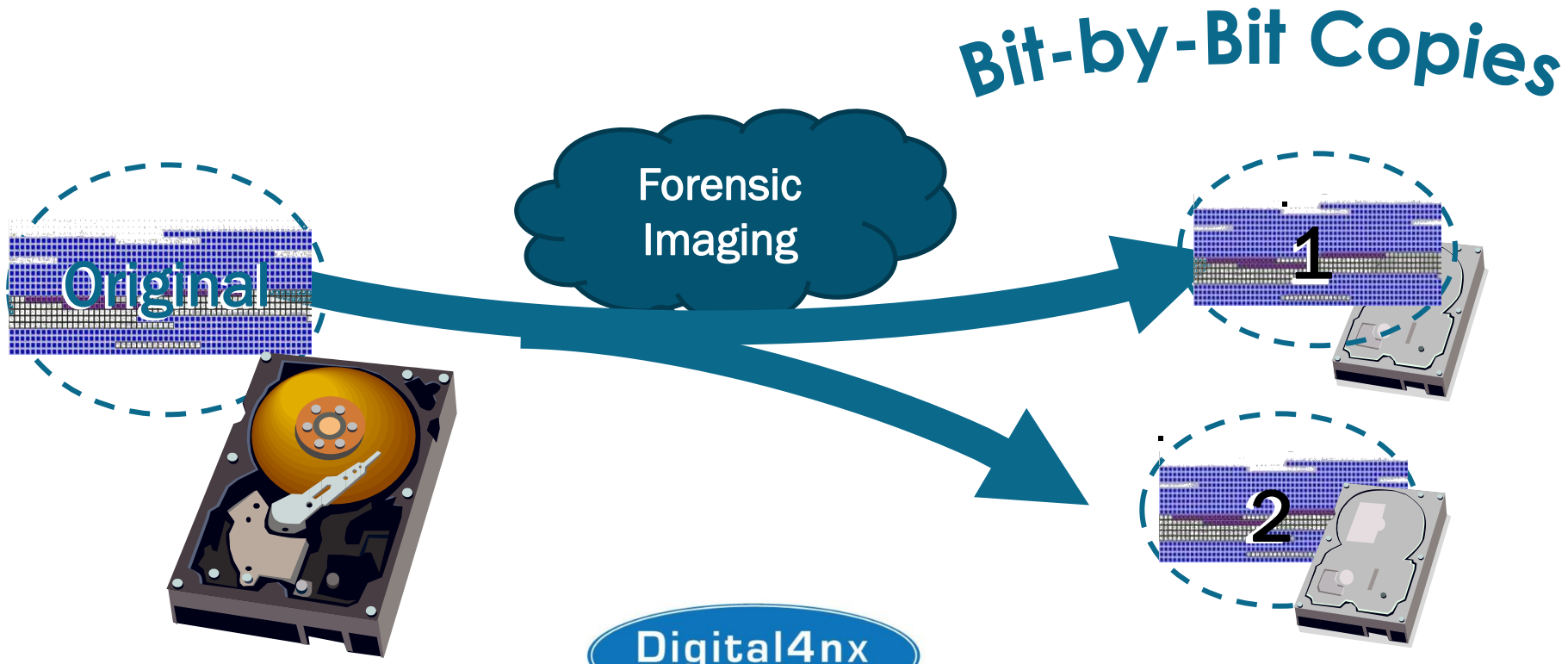


Digital4nx GROUP

...Bridging the Legal and Technology Gap

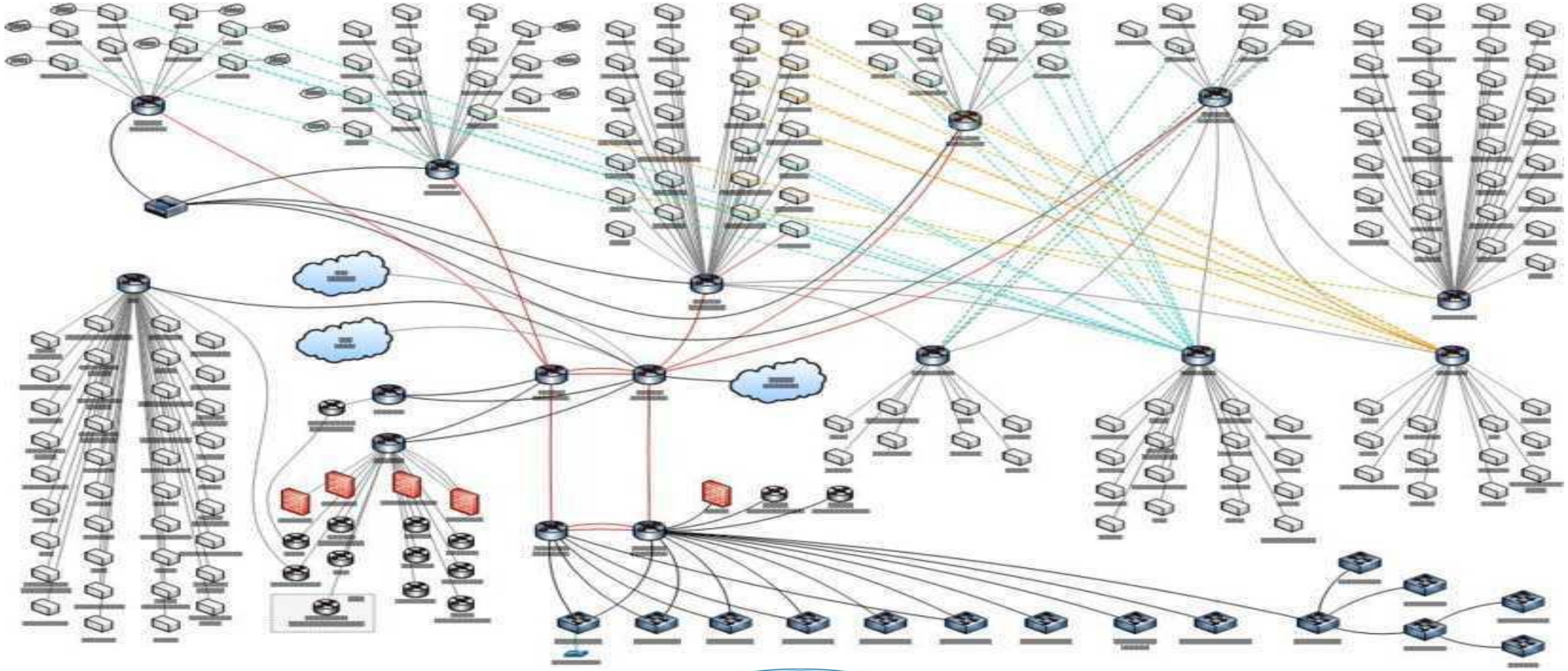
Preservation: Forensic Image

- Bit-by-bit copies of original data.
- Exact representation of original evidence.
- The original evidence is NOT modified.



Digital4nx GROUP
...Bridging the Legal and Technology Gap

Do You Know Where Your Data Is?



Digital4nx GROUP

...Bridging the Legal and Technology Gap


Everyone Has A Plan Until They Get Punched In The Mouth
– Mike Tyson

Areas of Practice

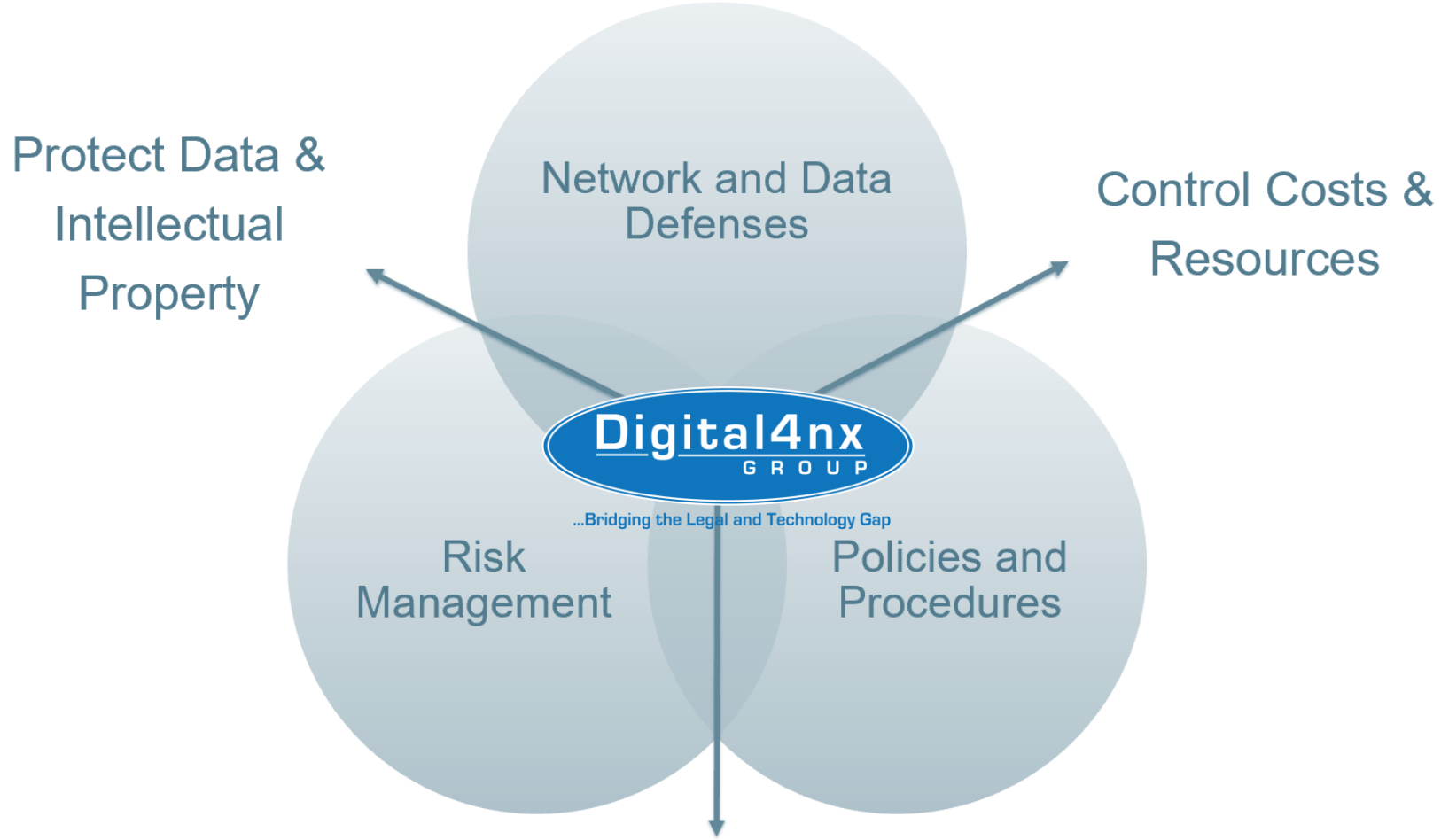
We help businesses stop kicking the can down the road and help them adhere to their Contractual, Regulatory, or Compliance Obligations through our advisory offerings:

- ❑ **Advanced Ethical Hacking**
- ❑ **Cyber Risk and Compliance Assessment**
- ❑ **Employee Awareness Programs**
- ❑ **Post Breach Incident Response**

Digital4nx GROUP

...Bridging the Legal and Technology Gap

Cybersecurity Risk Mitigation



Digital4nx GROUP
...Bridging the Legal and Technology Gap

"You Will Be Sued"

Digital4nx GROUP

...Bridging the Legal and Technology Gap

Bridging the Legal and Technology Gap since early 2000's

Rob Kleeger – Managing Director

D. 973-699-0167

E. rkleeger@digital4nxgroup.com

Are Your Best Relationships Prepared For Being Punched In The Mouth ?

ANY QUESTIONS

Digital4nx GROUP

...Bridging the Legal and Technology Gap

Rob Kleeger is the Founder and Managing Director of Digital4nx Group, Ltd. Rob is a subject matter expert on digital forensics, cyber security, and electronic discovery. Rob has overseen several leading digital evidence matters since being involved in this emerging field since its inception in the private sector such as **Zubulake v. UBS Warburg (The leading eDiscovery case), The 1st criminal case from The Enron Scandal, and Sony Computer Entertainment America, Inc. v. Hotz (The hacktivist group Anonymous)**. Rob was a Senior Partner in a leading Digital Forensics firm managing strategic relationships and directing case management teams, sales teams until the firm was acquired by a global business risk advisory and compliance firm in early 2006.

Rob collaborates with SMB business owners/leadership, attorneys, investigators, IT professionals, financial executives, human resource and compliance leaders who need a reliable partner to systematically identify, preserve, extract, analyze, and interpret digital evidence. In addition, Rob has led and managed such engagements as privacy assessments, information technology (IT) controls assessments, vendor security assessments, cyber risk assessments, information security consulting and project management.

In his current role, Rob works with organizations in different industry verticals including consumer product and retail, financial services, health sciences, real estate, investment firms, manufacturing and distribution, technology, and many more. Rob helps organizations adopt industry best practices and frameworks to improve efficiencies in day-to-day processes and identifies IT governance initiatives that help corporations and organizations enhance their existing IT environment. Rob assists IT department executives with their information assurance, IT strategy, and information security initiatives.

Rob is a respected educator in the field and regularly provides lectures on issues regarding cyber security, digital forensic investigations, and the production of electronically stored information to law firms, litigation professionals, business executives, various industry organizations and many other conferences and seminars in the New York Metro area as well as nationally, and has been featured on WNBC/NBC 4 News Channel.

Digital4nx Group provides a blend of legal and technology services to Lawyers, Business Owners, IT Professionals, Financial Executives, Trusted Advisors, and Human Resource and Compliance leaders who need a reliable partner to systematically identify, preserve, extract, analyze, and interpret digital evidence. This multi-disciplined approach leverages our strength to provide services such as:

Cyber Security Services:	Digital Litigation Support Services:
Advanced "Ethical Hacking"	Digital Forensic Investigations
Incident Response to Cyber Incidents or Data Breaches	Electronic Discovery Hosting, Consulting, and Advisory
Cyber Security Awareness Training	Expert Witness Testimony

Digital4nx Group's team possesses various certifications: Certified Computer Examiner (CCE); Certified Forensic Examiner (CFE); Certified Ethical Hacker (CEH); GIAC Penetration Tester (GPEN); Offensive Security Certified Professional (OSCP); Microsoft Certified Professional (MCP).

Digital4nx Group, Ltd.
8 S. Main St - Unit 70,
Marlboro Township, NJ 07746

Phone: 732-786-4062
Website: www.Digital4nxGroup.com
Email: info@digital4nxgroup.com

...Bridging the Legal and Technology Gap

Digital Litigation Services

Digital4nx Group, Ltd. (Digital4nx) systematically identify, preserve, extract, analyze, and interpret digital evidence for all types of legal matters that involve electronic evidence.

Digital forensics is a unique combination of science and art. A digital forensic examiner uses active and deleted data, as well as, "system-generated information" to reconstruct the timeline used by an individual behind the keyboard.

Our digital forensic examiners analyze files and artifacts that are left behind on storage media even after being copied, deleted, or compromised. Throughout our extensive analysis, we strictly comply with the rules of evidence.

If and when required to present or refute electronic evidence in a court of law, our experts at Digital4nx will testify on your behalf to explain our findings.

We have proven our ability to educate any judge, jury, opposing counsel, and our clients to understand the evidence obtained from our digital forensic examination. We provide litigation support services for Plaintiffs or Defendants, as well as providing expert testimony and consulting, both in and out of court.

Digital Forensic Investigations and Expert Testimony	Early Case Assessment - ECA
The type of digital forensic matters we have experience with include a vast range of crimes facilitated by computers, such as: Data theft, Restricted Covenant & Non-Compete, Sexual Harassment, Discrimination, Theft of IP, Commercial Litigation, Embezzlement, Bankruptcy, FINRA/SEC/HIPAA Inspections or Violations, Securities Fraud, Matrimonial Related Matters, White Collar Crime, and many more. Digital4nx's experts have advised countless clients across the US and routinely: • Help identify the locations, custodians, and methods utilized in storing electronic information; • Preparing preservation protocols, requests for production, meet and confer conferences for electronic discovery in litigation; • Coordinating the preservation, collection, and extraction of potentially discoverable ESI; • Preparing discovery requests and responses; • Working with litigation teams to efficiently review and analyze documents for production and trial preparation.	Conducting an ECA on a storage device (i.e., computer, tablet, cell phone, USB, etc.) may establish a user's various trends such as installation of programs, mass deletions of files, as well as link files which may provide details of the directories a particular file was accessed from. It may also provide whether or not a file has been accessed, copied, and/or otherwise tampered with from a shared computer or company directory (i.e., corporate server). Our Team can also determine whether an unauthorized program was installed, such as a data-wiping program, as well as being able to do much more. We assist litigation counsel and the client by analyzing and synthesizing evidence from multiple sources, collaborating with our client and their counsel to develop an initial case strategy while also formulating a preliminary discovery and litigation plan that will advance the chosen strategy towards a successful resolution. Cases are won by identifying clear litigation objectives and from there building a litigation plan that is focused on achieving those goals.

Digital4nx Group, Ltd.
8 S. Main St - Unit 70,
Marlboro Township, NJ 07746

Phone: 732-786-4062
Website: www.Digital4nxGroup.com
Email: info@digital4nxgroup.com

...Bridging the Legal and Technology Gap

ProActive Cyber Security Services

The reality for small and mid-sized businesses is they are increasingly the primary targets for criminals and hackers looking to gain access to critical assets, customer information, intellectual property, and financial data. This continuous cyber threat has put increased pressure on organizations to take a strategic look at risks associated with their cybersecurity practices, policies, and procedures.

Digital4nx Group, Ltd. (Digital4nx) brings the right mix of business knowledge and cybersecurity expertise to enable companies to make informed cyber-based decisions, with a detailed roadmap allowing them to prioritize the steps necessary to mitigate cybersecurity-related risks, allowing their businesses to grow. Digital4nx provides companies with an independent third-party assessment executed by our team of cyber experts. As a trusted advisor to organizations of all sizes, Digital4nx helps align security programs with business priorities, regulations, and risk appetite.

In short, we guide Business Leaders through the journey of being "Reasonable and Defensible" by providing information to make informed decisions around how they secure and manage data, operate their business and provide a risk framework around the data, and enhancing their overall cyber security.

Ala carte services :

Advanced Ethical Hacking:	Cyber Risk Assessment:
This is not simply a penetration test. Our Security Team will use high-level techniques to test your network or web applications to the level of an Advanced Persistent Threat (APT). An APT is a sustained and targeted attack that uses high-level and covert tactics. These attacks can cause extreme damage and are very difficult to detect and defend against. This is one of the areas where Digital4nx's team excels over the competition. Rather than just scan and test your network with traditional penetration testing software, our team of high-level ethical hackers use manual and advanced techniques to test to the highest level of attacks, ensuring your network is fully secured. The goal of an "advanced ethical hacking" is to provide business leaders with a road-map for making the network much more secure, identify the sensitive information aka "crown-jewels" which the organization maintains, and improve the best reasonable and defensible security measures for leaders to make informed decisions.	Digital4nx's Cyber Security Risk Assessment (CRA) is customized to meet your organization's specific needs, assessing cyber-related risk based on your company's industry, regulations, objectives, and threshold for risk. Our process is designed to help business leaders determine where Cyber Security risks could impact a business's bottom line. We design our CRA from a cybersecurity framework that ensures effective compliance, risk and delivers compliance incorporates all the requirements of many data security regulations, industry standards, and requirements such as the NIST Cybersecurity Framework, CIS Critical Security Controls, ISO27001, CMMC, NY DFS CR500, PCI, GDPR, HIPAA, etc.

Digital4nx Group's team possesses various certifications: Certified Computer Examiner (CCE); Certified Forensic Examiner (CFE); Certified Ethical Hacker (CEH); GIAC Penetration Tester (GPEN); Offensive Security Certified Professional (OSCP); Microsoft Certified Professional (MCP).

Digital4nx Group, Ltd.
8 S. Main St - Unit 70,
Marlboro Township, NJ 07746

Phone: 732-786-4062
Website: www.Digital4nxGroup.com
Email: info@digital4nxgroup.com

The Threat From Within – Theft of IP

Zach grew up in the family business. After college, he began working for the company and during his eighteen-year employment at MedSoftCo, Zack worked hand in hand with the Company's development team in developing and enhancing MedSoftCo's scheduling software application and had direct access to source code underlying the software. In early 2021, Zack was promoted to the role of Director of Product Management, a senior level position, which included a minority equity position in the business..

In his new role, Zack had access to numerous high level and key company documents, data and databases, including the MedSoftCo GitHub repository containing the highly confidential source code for its scheduling software. Zack was no longer responsible for coding and thus had no reason to work on source code. In fact, the Company expressly instructed Zack to discontinue working on the source code

Zack's new job responsibilities included:

a. Driving MedSoftCo technology, new products and offerings, pricing strategies, and technology roadmap to insure Plaintiff's competitive advantage in the market;

b. Working as the face of the MedSoftCo platform for both internal and external stakeholders;

c. Managing both strategic and tactical activities for MedSoftCo's technology;

d. High-level interaction with MedSoftCo users including focus groups, one-on-one conversations, user groups, among other methods;

e. Management of all market and technical problems, requirements, and system requirements;

f. Organizing and leading user testing programs for MedSoftCo technology, including internal alpha and external beta programs; and

g. Working closely with the MedSoftCo corporate team to establish technology budgets, activities, and investments.

Zack resigned from MedSoftCo on February 12, 2022 and that he was going to work for a competitor.

MedSoftCo contacted their attorney who retained Digital4nx Group. Digital4nx began an early case assessment — ("ECA") of his company owned devices and quickly learned of his unauthorized activities.

Digital4nx Group, Ltd.
8 S. Main St - Unit 70,
Marlboro Township, NJ 07746

Phone: 732-786-4062
Website: www.Digital4nxGroup.com
Email: info@digital4nxgroup.com

The Threat From Within – Theft of IP

The results of the ECA revealed:

- In as early as April 2021, Zack began installing software to download the MedSoftCo scheduling software source code to his own computer against company policy.
- Zack accessed the MedSoftCo GitHub repository to download approximately fifty thousand (50,000) files containing MedSoftCo source code onto his OneDrive cloud system and his computer's local C Drive.
- The ECA also revealed that less than a month prior to his resignation (January 2022), he began the interview process with CompetiSoftCo
- Zach's conduct of downloading the source code continued on the same days he gave verbal and written notice of his resignation, 2/12/22, 2/14/22 and 2/24/22. NOTE: The majority of the file downloads occurred during non-working hours on weekends.

- The ECA's internet searches revealed that after Zach gave notice of his resignation, two key indicators of his intentions to misappropriate source code became apparent.
  - First, Zack reviewed a software article entitled "Who Owns the Code?" which explains the issues associated with efforts of source code programmers to reuse code they had developed after moving to a new employer.
  - Second, Zack conducted a search to determine how to create remote work access for a separate (non-MedSoftCo) computer, enabling him to log into that computer and remotely access MedSoftCo systems. (Links from Zack's Google Chrome Browser).
- Zack also used his MedSoftCo issued work phone to communicate with CompetiSoftCo and to schedule his Zoom interviews with CompetiSoftCo's reps.
- The calendar entries obtained from Zack's work phone reflect that from January 20, 2022 through February 8, 2022—the very time period during which Zack was downloading the source code — Zack engaged in multiple Zoom calls with CompetiSoftCo senior management, including its CEO.
- After his CompetiSoftCo offer was emailed to his personal Gmail address on February 8, 2022, Zack texted a coworker, boasting about his decision to leave MedSoftCo: "I'm gonna give them 6 weeks notice and moonlighting after."
- On February 13, Zach used a series of external USB devices—used to store and transfer data from one device to another (i.e., computer to computer transfer of files)—to connect to his devices, which were not disclosed or returned to MedSoftCo when his employment ended.
- In addition to Zack having access to numerous external devices, he backed up to platforms including a Google Gmail address, additional phone, Dropbox, and a Google Drive account linked to his MedSoftCo Devices.

A complaint was filed against Zach and CompetiSoftCo with a panoply of federal and New Jersey laws, including without limitation the Federal Defend Trade Secrets Act, codified at 18 U.S. Code § 1836, and the Computer Fraud and Abuse Act, codified at 18 U.S.C. § 1030), as well as a violation of the Non-Disclosure and Non-Competition Agreement ("NDA").

To date, CompetiSoftCo has agreed that it never expressed to Zach to steal any source code. CompetiSoftCo has also agreed to cooperate in the investigation to determine if any MedSoftCo exists on their network.

The investigation is still ongoing.

Digital4nx Group, Ltd.
8 S. Main St - Unit 70,
Marlboro Township, NJ 07746

Phone: 732-786-4062
Website: www.Digital4nxGroup.com
Email: info@digital4nxgroup.com

When The Hack of a Business Partner is Just as Bad as the Compromise of Your Own Systems.

Digital4nx was recently retained in a post-incident response investigation of a highly targeted spear phishing email attack. Based upon the available evidence and confirming with LifeScienceCo ("LSC"), the attack began on or around January 25, 2022. The victims targeted were between the LSC's Assistant Controller and the accounting supervisor of their Client.

The attack succeeded in having Client divert an approximate $730,000 payment of legitimate invoices to a fraudulent bank account. The attacker appeared to have used a common BEC – Business Email Compromise techniques possibly executing a carefully planned man-in-the-middle (MITM) attack.

The attackers use of the lookalike domains technique, present a severe threat. Not only to the originally attacked organization but also to the third-parties with whom they communicated using the lookalike domain. Typically, the attack scheme works by sending phishing emails to high profile individuals in the target organization to gain control of the account and carry out extensive reconnaissance to understand the nature of business and the key roles inside the company.

As in this case, the attacker sent one mail each from the spoofed domains to the counterparty, thus inserting itself into the conversation and deceiving the recipient into thinking that the source of the email is legitimate.

The attacker sent one mail each from the spoofed domains to the counterparty, thus inserting itself into the conversation and deceiving the recipient into thinking that the source of the email is legitimate.

In essence, the attacker poked each victim in the chest a little…knowing the attempted scam was being executed.

The emails that we examined point to the fact that the attacker behind the domains were in possession of information regarding possible financial transactions between our Client and Their Client. The examination of our LSC's servers and involved computer did not reveal any compromises, malware, or intrusions. Additionally, there was nothing to suggest that data was exfiltrated from LSC's network.

The attack began communicating with their client several days before engaging with LSC, and the fact that LSC did not share any banking information lead us to conclude that it is more likely than not, that LSC's Client's network systems were compromised and caused LSC's Client to wire money to the intruders' account.

In this case, Not only did LSC incur costs to provide the posture that Digital4nx, conducted an independent investigation and provided an opinion to support LCS in their claims against their Client who not only has still not paid our Client the $700K, but their Client was negligent and out $1.4M.