ANATOMY OF CYBER CASE

1. **Discussion of Insider Threat (M. Pirtle)**
2. **Discussion of 18 U.S.C. § 1030 (P.Hull)**
3. **Scenario Introduction (D.Ries)**
4. **Investigation**
    a. **Incident Discovery by Victim:**
        i. Civil Perspective: discussion with internal counsel and outside counsel (D. Ries)

        ii. Victim Expert to investigate and Re-Secure System
            1. Determine method of infiltration
            2. Determine what information and systems were affected
            3. Determine what data was taken
            4. Determine method of exfiltration

        iii. Legal Notification issues

        iv. Discussion with Civil Counsel as to whether to notify Law enforcement

        v. Preparation for LE contact
            1. triage - preserve evidence of malware/ image affected computer systems using good forensic techniques
            2. preservation of evidence related to criminal violation:
                a. logs showing damage done
                b. Identify number of affected computers
                c. Provide copy of malware
                d. logs of exfiltration method of data and location
                e. Any clues identifying the intruder
                f. Costs associated with the intrusion

    b. **Call to Law enforcement**
        i. Victim/LE conference (P.Hull & M.Pirtle)
            1. LE obtains evidence: forensic copies of affected media, malware, records of costs, and any logs showing infiltration (phishing email or location of infected sites), damage, or exfiltration
            2. for insider case, suspects from victim
            3. LE will want corporate policies, corporate handbooks, computer handbooks or human resources policies

        ii. Evidence Gathering Tools (P.Hull)
            1. grand jury subpoena for documents requires no probable cause showing to a judge, but is limited to a third party's records and just subscriber information from an internet service provider
            2. 2703d orders requiring the production of logs from ISPs/hosters. It requires that an application be made

to a magistrate judge demonstrating specific and articulable facts that make it reasonable to believe that the information sought is relevant and material to an ongoing criminal investigation.

3. search warrant under 2703 for email or other content less than 180 days old which is stored on an ISPs computers or
4. a search warrant for computers within a premises under Rule 41
5. Both require a showing of probable cause before a magistrate judge
6. It is routine in criminal investigations to obtain court orders sealing legal process
7. It is also routine where a particular ISP has a policy of notifying the customer about an evidence in the form of a search warrant or court order to obtain orders directing non-disclosure
8. Real-time Legal Process: pentrap to determine the locations of communication the legal standard is certification of relevance by the prosecutor and wiretap to intercept actual content or conversations the legal standard is probable cause
9. MLAT request may be made to obtain the same types of information for accounts overseas – the standard is to demonstrate relevance of certain information and/or provide heightened factual justification for the most intrusive process
10. grand jury testimony from witnesses

5. **Prosecution (P.Hull)**

a. Grand Jury Process (briefly)

b. Legal Problem areas with 1030

i. Auernheimer Venue

1. Proper venue within the judicial district is required in order to bring a prosecution

2. Government must prove venue by a preponderance of the evidence

3. Applying the principles of venue to network crimes is not always a straightforward endeavor. Especially when considering crimes that involve intrusion which takes place at computer facilities stored in the cloud. Those facilities could be located outside of the district or the country while the headquarters or the unit of the business who interacts with the data could be in the district.

4. The central inquiry in venue analysis is determining where the crime was committed. The exact location of each event—the "accessing" and the "obtaining"— may not always be easily determined.

5. None of the intrusion crimes contain a specific venue provision.

6. The Supreme Court cases indicate that venue should lie in the district where essential conduct elements of the crime occurred. U.S. v Rodriguez-Moreno, 526 U.S. 275, 280 (1999).

7. Currently, there is a case in the United States Court of Appeals for the Third Circuit which raises the issue as to whether venue may lie in the district where there are substantial contacts from the crime such as the effect of the crime. That is a question left open by the Supreme Court.

   a. US v Auernheimer which also raises interpretation questions such as whether there is indeed an unauthorized access when the website that is available to the public allows access to confidential information to one group but does not have strong security preventing others from changing the settings of their computer and entering a specialized term to the web address to gain access to the confidential information as if the interloper was part of the group granted access.

   b. US v Auernheimer which raises the issue of what proof is necessary to raise a 1030 misdemeanor to a felony

ii. Nosal Problem "exceeds authorized access"

1. Explain Nosal factual scenario

2. 18 U.S.C. § 1030(e)(6): "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter"

3. Circuit split--
   a. Ninth: United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc)("exceeds authorized access" in § 1030(e)(6) "is limited to violations of

restrictions on access to information, and not restrictions on its use")

b. Fourth follows Nosal: WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012)

c. Fifth, Seventh, and Eleventh Circuits come out the other way

i. United States v. John, 597 F.3d 263 (5th Cir. 2010); Int'l Airport v. Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006); United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010)

4. The rest: no authority one way or the other

a. It appears that, though the Third Circuit has not addressed the question, the district courts within the circuit are pretty uniformly taking the same approach as the Ninth Circuit.

b. Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610, 621 (E.D. Pa. 2013).

c. Robinson v. New Jersey, CIV. 11-6139, 2013 WL 3894129 (D.N.J. July 26, 2013).

d. Carnegie Strategic Design Engineers, LLC v. Cloherty, CIV.A. 13-1112, 2014 WL 896636 (W.D. Pa. Mar. 6, 2014).

e. Given the narrow interpretation of the term exceeds authorized access, we would be considering other theories/offenses such as 18 USC 1341 and 1343; 18 USC 1831 et seq; and export control offenses

iii. Political/Altruistic Motives as a Defense

1. Are such Motives relevant to Mens Rea of the 1030 Offenses

a. Our contention would be that altruistic feelings that motivated the commission of a crimes are not relevant to determining the existence of the requisite knowledge and intent required by the 1030 crimes most applicable to this fact pattern

b. If evidence shows that intruder acted knowingly or intentionally to gain unauthorized access or exceed authorized access to the protected computer, that evidence completes the crime

c. Whatever the motive was to commit the crime we would contend that it is irrelevant to the question of violation of the criminal provision

i. Example cases so holding are U.S. v Malinowski, 472 F.2d. 850, 853 (3d Cir 1973); Roe v. Operation Rescue, 919 F.2d 857 (3d Cir. 1990); U.S. v Romano, 849 F2d. 812, 816 n.7 (3d Cir 1988); U.S. v. Bailey, 444 U.S. 394, 100 S.Ct. 624 (1980)

d. Few criminal offenses use purpose and motive as an element of the crime. There is no nexus between the intrusion and preventing perceived wrong.

2. The altruistic motives do not meet the requirements for justification, duress, and necessity affirmative defenses

a. While altruistic motives do not negate the existence of intent or knowledge under 1030, our contention would be that the defense is trying to use them to excuse the criminal act as an affirmative defense. See Dixon v. United States, 548 U.S. 1, 8, 126 S.Ct. 2437, 2443, 165 L.Ed.2d 299 (2006)

b. That evidence only comes in if it can meet the test of the affirmative defense of necessity and justification. It does not.

c. Justification or necessity or choice of evils is traditionally described as a situation where physical forces beyond the actor's control rendered illegal conduct the lesser of two evils. Thus, where A destroyed the dike in order to protect more valuable property from flooding, A could claim a defense of necessity. U.S. v. Bailey, 444 U.S. 394, 100 S.Ct. 624 (1980)

d. Under any definition of the necessity or justification defenses one principle remains constant: if there was a reasonable, legal alternative to violating the law, "a chance both to refuse to do the criminal act and also to avoid the threatened harm," the defenses will fail. Id at 410-11, 635; U.S. v. Miller, 59 F.3d 417, 422 (3d Cir. 1995)

e. We would suggest that the defense cannot satisfy the requirement that committing the intrusion was the only reasonable alternative to the condition that the defendant cites as the motive for committing the crime, it is a greater evil, and it

is not directly linked to resolving the perceived evil.

3. Is evidence of altruistic motives excludable from evidence

   a. Our contention would be that the evidence should be excluded because it is irrelevant and unfairly prejudicial.

   b. We would file a motion in limine to exclude evidence of altruistic motives.

      i. The evidence of motive here would not only be irrelevant to the issue of mens rea, but would itself have an undue tendency to suggest that the jury's decision should be made on basis not supported in the law such as sympathy for the cause of the defendant. Carter v. Hewitt, 617 F.2d 961 (3d Cir 1980).

      ii. We would utilize F.R.Evid. 403 to exclude the evidence