Information Assurance Final Paper

Jonathan Roeseler

Old Dominion University

CS 465: Information Assurance

Professor Hao

May 12, 2026

CIAO Report: DNC Breach

Summary

Around April 2016, advanced persistent threat [APT] actors, closely affiliated with Russia, named APT28 (Fancy Bear) and APT29 (Cozy Bear), infiltrated the Democratic National Committee (Naseer, 2024). This hacking campaign against the DNC, in addition to other operations, including disinformation dissemination, was part of a Russian scheme designed to influence US election outcomes. The operation demonstrated the impacts of poor cybersecurity practices in networks critical to maintaining trust in political institutions. I will describe the DNC, the consequences of this incident, and offer an assessment and path forward for the organization to move securely in the future.

DNC Background

The Democratic National Committee, more commonly known as the DNC, is the backbone of the Democratic Party, one of the two large parties that ultimately govern America. The DNC coordinates the Democrats' national strategy, organizing events, fundraising, and conducting polling, among other tasks that further the party's ideals. The committee also oversees the branding and serves as a platform for the party, comprising numerous digital systems and applications. The DNC has alliances throughout the government, media, technology, and the private sector (including individuals). These alliances are necessary to fund candidates, optimize strategy, and deliver content to voters.

Consequences

The DNC’s reputation was severely tarnished as a result of this incident. Sensitive data was lost and published for the world, severely hampering the DNC’s efforts in the 2016 election. Entire networks had to be rebuilt, causing downtime when there was none to be lost. The breach

also serves as a catalyst for national counter-disinformation campaigns by organizations like the FBI, among other US agencies. The hack demonstrated the need for more robust security measures. The cyber impact was tremendous, as the DNC had to consult a third party to lead remediation efforts. Furthermore, the incident caused massive overhauls and recognition of supporting stronger standards and systems to prevent similar attacks, including MFA and regular patching (Naseer, 2024).

Vulnerability Assessment

The DNC has numerous assets that allow it to fulfill its mission. The table below will map assets based on their importance to the organization and the IA requirements of the asset: confidentiality [C], integrity [I], availability [A], and non-repudiation [N].

Asset	Importance	IA Requirements
Identity / Network Infrastructure	Critical	C,I,A,N
Email Services	Critical	C,I,A,N
File / Document / Database Repos (Containing critical data)	Critical	C,I,A,N
Financial Systems & Services	Critical	C,I,A,N
Public Sites	Essential	I,A
Collaboration Tools	Essential	C

Social Media	Essential	A
Other Marketing Tools	Ancillary	A

The attack impacted many of the critical assets listed above. The investigation of this incident determined several vulnerabilities related to some of these assets, severely impacting the confidentiality, integrity, availability, and non-repudiation of critical assets. A vulnerability assessment of the DNC's network would have identified the following: outdated or improperly secured email server(s), poor identity management and access control (enabling lateral movement and privilege escalation), inadequate user training, and inadequate endpoint security. These vulnerabilities, when combined, form a chain of easily exploitable processes, at least within the initial access phase, considered simple for even novice hackers – in the DNC case, they had state-sponsored actors in their systems. The attack proved that even a less sophisticated adversary may have pulled off a similar result. An assessment run before the attacks occurred would not only have identified these vulnerabilities, but it would have called for measures and controls to fix these weaknesses instantly. In their environment, where political institutions are consistently attacked, vulnerabilities like outdated servers or signatures are absolutely unacceptable.

According to CrowdStrike, the attack played out as follows: 1) attackers exploited outdated or not appropriately secure email servers, followed up by a spear-phishing campaign to gather credentials of certain personnel. 2) The phishing emails also downloaded sophisticated malware, enabling persistence within the network. 3) Attackers relied on weak identity security measures, such as poor MFA and password hygiene, to further gain elevated privileges and move laterally around the network. They utilized credential dumping tools (Indicating poor endpoint

and identity security policy). 4) Once persistence and privilege escalation were achieved, the actors were able to extract documents from internal servers. It is important to note that at step one, the breach of an email server and even just one account accessed is a significant attack, especially if sensitive emails are not being applied secure policy (encryption/digital signatures) or protected by MFA. If MFA and encryption on critical emails were done properly, and assuming the attack stopped there, much of this threat could have been stopped; however, the "Prevention" section of this paper will highlight more of how to truly stop these attacks. The assessment would have identified many of the steps taken in the attack, from the outdated email server (1) to poor identity security (1,3) and inadequate endpoint security (2,4).

Threat Matrix

After identifying the vulnerabilities of these assets, a matrix may be constructed to better determine where controls should be prioritized.

THREAT	ASSET	LIKELIHOOD	IMPACT	RISK LEVEL
Social Engineering (Phishing, BEC)	Users & Email	HIGH	HIGH	HIGH
Credential Theft	Identity Infrastructure & Users	HIGH	HIGH	HIGH
Lateral Movement & Privilege Escalation	Internal Network	MEDIUM	HIGH	MEDIUM

Data Exfiltration	Critical Data, Email	MEDIUM	HIGH	MEDIUM
DDoS	Public-Facing Services & Sites	MEDIUM	MEDIUM	MEDIUM
Zero-days	Network & Financial Infrastructure	LOW	HIGH	MEDIUM

From this matrix, it is easy to tell that the likelihood of attacks on DNC assets is going to be much higher than that of other organizations. This is because of the implications of a compromise and the value of DNC data, such as the potential to swing elections, and because political organizations are much more likely to be targeted by attacks. Akshay Joshi cites a study showing that state institutions and political systems are the second most targeted in cybercrime attacks.

Phishing is the most common cause of data breaches and the most costly. As the attack is incredibly common, the likelihood of such an attempt is rated high. Furthermore, as phishing is the leading initial access vector for complex breaches, the impact of a successful attack can vary, but in an environment that requires secrecy, the impact of a successful attack is high. Crowdstrike's incident report determined that spear-phishing, a type of phishing where specific users, usually those with more access or seniority, are targeted, was the initial access vector in the DNC breach.

Credential theft is another very common form of attack. This attack relies on poor identity protection to truly succeed. There are a variety of ways to steal one's credentials, in the DNC's case, at least two different types were performed: stealing via phishing links and harvesting offline once they gathered the passwords of elevated accounts. The likelihood and impact of any credential theft threat is high, especially in an environment like the DNC, where little or no loss should be tolerated. A variety of technologies are required to mitigate this threat, which will be discussed in the "Prevention" section.

Lateral movement and privelege escalation are two threats that must be identified and prevented. These threats can enable ransomware, leaving networks offline forever, demonstrating the high impact rating. The likelihood of such an attack is medium. The attack usually will require some sophistication, but poor identity protection policies, such as poor password management, not separating admin privileges from user accounts, and so on, easily enable this attack.

Data exfiltration is another common threat most organizations have faced. This threat may materialize in many ways, such as from outside threats and inside threats, and sometimes even accidentally. In our case, it was an outside threat. Poor or non-existent data protection, such as labeling. and data loss prevention tools enabled this attack to be carried out successfully. The impact of highly confidential documents being leaked is tremendous, thus the High impact rating.

Denial of Service is a medium risk to the DNC. Although not as common as the other attacks, its impact can affect availability, which is crucial to their mission. Offline websites and services in an election cycle can cause huge reputational and strategic damage. There was no DoS or DDoS attack in the 2016 breach.

Zero-days are incredibly rare, yet sophisticated attacks. Many times, these attacks have a tremendously high impact, enabling full network compromises in some cases. As a result, impact is determined to be high, but the likelihood is low. When zero-days are found, patching or isolating affected systems is crucial. Although the DNC was breached in the attack by outdated software (not a zero-day) in their environments, it demonstrates that patch management and defense in depth are necessary for their operational security.

Communication Plan

An effective communications plan is necessary for mitigating cybersecurity incidents. The goal of the plan is to quickly identify teams and stakeholders who should be notified when an incident is declared. A formal document outlining the teams and their objectives, as well as their contact information, shall be made. Furthermore, this document should list who is responsible for the internal and external communications. The document should serve to protect the organization's interests while maintaining compliance with applicable laws. Finally, the document should list appropriate messaging channels and aim to reduce spillage, in order not to spread sensitive information as well as misinformation. The plan should be tested before real incidents occur. This will help in identifying any gaps in the plan.

An example plan:

The Incident Response team is responsible for approving all communications regarding the incident. Their goal is to coordinate with proper IT and Cyber teams, Legal, and Leadership to resolve an incident. The legal team is responsible for ensuring the organization stays in compliance with laws regarding breach notifications. They are helpful in identifying what MUST be said to respective parties. The IT and Cyber teams are responsible for investigating the

incident and determining the technical steps forward to remediate. They may also advise on policy changes to prevent recurrence.

The internal communication plan focuses on ensuring that proper teams and stakeholders are notified of an incident. It will have a list of each department's contact information. A hierarchy is also established. This plan will ensure a “locked down” Teams or Email channel is created with the proper teams to ensure the incident is covered from start to finish.

The external communication plans focus on contacting respective parties in the event an incident requires third-party remediation efforts or notification. This may include third-party incident response and cyber teams, as well as a list of contacts in government to declare a breach occurred in accordance with reporting laws.

Prevention

There are a variety of ways the DNC could have contained the attack or even outright prevented it. First, the threats from the threat matrix that were relevant in the DNC breach will be discussed, along with their appropriate mitigations. Then, an overarching architecture and policy design to employ a strong security posture will be discussed.

As the DNC breach ultimately compounded as a result of social engineering, specifically phishing, the need for communication security is paramount to the organization's success. A defense-in-depth approach should be used, where there is a primary security email gateway that blocks threats from the outside, such as Mimecast, and a secondary gateway that “sits” behind the primary email gateway that runs checks of its own and is optimized for internal use (Exchange). This setup ensures that emails are scanned at least twice by two different platforms, but it also ensures that investigations can be run on either in the event one of the systems is offline or compromised. These systems would scan both links and attachments for malware, in

addition to the message itself. Phishing is the easiest and most common initial access vector, therefore other measures must be taken as well. Utilizing phishing-resistant authentication, such as FIDO2, further prevents and mitigates many phishing attempts. Strong identity protection must be implemented, such as monitoring for suspicious sign-ins to prevent malicious logins. A common implementation of this is whitelists and conditional access policies. Another method that should be implemented is strong endpoint security, such as configuring what attachments may be opened, for example, a common block is macros on Excel and other documents. Endpoint security would include utilizing and scanning these links and attachments (outside of the email security systems check) to ensure safety. Some other measures to ensure stronger security for the endpoint would be web filtering/proxy, DNS filtering, and strong and updated firewalls. These measures assume a malicious link or attachment will be downloaded or clicked, and upon a successful phishing attempt, the impact is minimized. Finally, training must be implemented for employees. Employees should be able to recognize phishing attempts and be able to easily report them to a security team. All of these methods ensure organizations stay safe from even the most sophisticated adversaries.

Credential theft is another common attack path for adversaries. The goal is to move laterally to ensure persistence is achieved, then elevate privileges to be able to take control over the network. There are many preventative measures to mitigate this threat. Enforcing the use of strong passwords, utilizing strong or phishing-resistant multifactor authentication, least privilege implementations, and monitoring the network for poor passwords and attacks. Least privilege implementation usually requires the most steps, but it is by far one of the most important to mitigate against credential theft. User and daily work accounts should be separated from privileged accounts, and privileged accounts should only be accessible from privileged

workstations. This setup ensures that even if a user is compromised, lateral attacks or privilege escalation attempts would fail because the administrator/privileged accounts are logically separated from any affected endpoints. Furthermore, these accounts should have stronger policies applied against them, such as enforcing phishing-resistant MFA, not being able to browse the internet, and so on. Password expiration would ensure that even if compromised, by the time it's cracked, a replacement has already been made. Ideally, adopting passwordless authentication methods like smart cards or FIDO2 would render these credential dumping tools useless. Finally, monitoring the environment for passwords and poor hashes (passwords), would be a proactive step in ensuring accounts are not at risk of credential dumping attacks. Implementation of these controls would support the DNC's mission of remaining online by being able to contain and identify credential attacks.

Lateral Movement and Privelege Escalation are methods used by adversaries to establish a lasting presence on a network, enabling them to carry out a range of attacks, from data exfiltration to ransomware. The prevention of these attacks is largely mitigated by implementing some of the previous mitigation methods mentioned, such as strong endpoint security controls, identity protection, and adopting a least privilege strategy. This attack can further be prevented with network segmentation, such as separating servers from workstations subnets, and administrator workstations from them both. This is commonly done with VLANs and Firewalls, ensuring that traffic is legitimate and privileged network areas cannot be pivoted to in the event of a breach. Furthermore, segmentation ensures that once an attack is identified, affected hosts are able to be easily quarantined and separated from the network until remediation has occurred. Further controls, such as network intrusion detection systems [NIDS], would have been able to identify and stop a breach. For example, a NIDS would have identified anomalous traffic

occurring on the DNC network, moved to close down and isolate the endpoint, and alerted an administrator of the attempt.

Data exfiltration tarnished the DNC's reputation, as emails and documents with many of their partners were leaked. Many organizations do not have any policy or system regarding Data Loss Prevention [DLP], which is unacceptable for the DNC, considering its mission and environment. DLP tools are able to detect breaches by identifying confidential data leaving (or attempting to leave) the network. Furthermore, these tools can help organizations identify their data and apply policy to their data based on tags like "Confidential" or "PII". By applying policy to these tags, organizations can define the expectations of the data, such as not allowing it to leave the network, be copied, or enforcing encryption and strong access control.

The DNC failed beyond just technical controls. The DNC lacked policy for many systems, as well as its overall environment. The DNC should have adopted a defense-in-depth posture, ensuring compromises are able to be identified and contained, and adopt a zero-trust architecture. In a zero-trust environment, everything is vetted, so a user randomly accessing troves of confidential information would be marked as suspicious, and administrators would be alerted, or a suspicious link is clicked or reported by a user, which instantly runs a playbook to remediate the incident, in addition to opening an incident ticket with the security team to investigate. These scenarios secure modern infrastructures, and the DNC lacked it entirely, and some…Assuming breach is the philosophy the DNC must take to prevent recurrence of this incident, especially as it was proven to be done by sophisticated adversaries (Naseer, 2024). The DNC should adopt frameworks to remediate risks, such as with its out-of-date email platform. The frameworks the DNC should consider to implement controls and manage risk are NIST SP 800-37 (RMF) and 800-53(Security Controls). These publications work in tandem to secure

organizations across the globe, including the US Department of Defense. It is a proven system, and when important environments, such as the DNC's network, are attacked daily by sophisticated groups, these documents aid in developing a proper, proactive security environment.

References

Naseer, Iqra. "The crowdstrike incident: Analysis and unveiling the intricacies of modern cybersecurity breaches." *World Journal of Advanced Engineering Technology and Sciences* 10.1 (2024): 728-733.

Joshi, Aksay. “These Are the Biggest Cybercrime Targets, and Other Cybersecurity News to Know This Month.” *World Economic Forum*, Apr. 2024, www.weforum.org/stories/2024/04/cybercrime-target-sectors-cybersecurity-news/.