Authentication system

- I would recommend using an LDAP protocol (such as Microsoft Active Directory) to maintain a directory of users, for authenticating their access to various systems. Authorization levels and permissions can be set at the user, role, and/or group level.
- Another useful authentication mechanism they can implement is Single Sign-On or SSO. This is an authentication concept that allows users to authenticate once to be granted access to a lot of different services and applications. Since reauthentication for each service isn't needed, users don't need multiple sets of usernames and passwords across a mix of applications and services. SSO is accomplished by authenticating to a central authentication server, like an LDAP server (recommended above). This then provides a cookie, or token that can be used to get access to applications configured to use SSO.
    - SSO is really convenient. It allows users to have one set of credentials that grant access to lots of services, making it less likely that passwords will be written down or stored insecurely. This should also reduce the overhead for password assistance support and removes time spent re-authenticating throughout the workday.
- I would also recommend they use SSO with multi-factor authentication. Users would need to enter secondary information (a one-time code sent via text message, a key displayed on a token that changes every 60 seconds, etc.) in addition to their password. Because SSO will allow them one-time authentication access to multiple systems, extra scrutiny and a higher authentication standard should be used with it.

External website security

- Get a signed SSL/TLS server certificate from a certificate authority for establishing secure connections with clients and customers over the internet.
- It looks like they will be handling customer payment/credit card information. Therefore, the company must adhere to PCI DSS standards. These are the major PCI DSS standards they need to adhere to:
    - The first objective is to build and maintain a secure network and systems. This includes the requirements to install and maintain a firewall configuration to protect cardholder data and to not use vendor supply default for system passwords and other security parameters.
    - The second objective category is to protect cardholder data. In this objective, the first requirement is to protect stored cardholder data. The second is to encrypt the transmission of cardholder data across open public networks.
    - They need to make sure that sensitive payment information isn't stored beyond the time it's required. Once payment is authorized, authentication data shouldn't be needed anymore and it should be securely deleted.
    - They need to maintain a vulnerability management program.
        - Protect all systems against malware and regularly update antivirus software or programs.
        - Develop and maintain secure systems and applications.
        - Ensure all systems have antivirus software installed and this software is kept up to date.
        - Require that scans are run regularly and logs are maintained.
        - Ensuring systems and software are protected against known vulnerabilities by applying security patches at least one month from the release of a security patch.
        - Use of third-party security vulnerability databases is also listed to help identify known vulnerabilities within managed systems. Implement strong access control measures.
    - Restrict access to cardholder data by business need-to-know.
        - Identify and authenticate access to system components.
        - Restrict physical access to cardholder data.
    - Regularly monitor and test networks.
    - Track and monitor all access to network resources and cardholder data.
    - Regularly test security systems and processes.
    - Setting up and configuring intrusion detection systems and conducting vulnerability scans of the network
    - Maintain an information security policy - maintain a policy that addresses information security for all personnel.

Internal website security

- A recommendation would be implementing a RADIUS server to centralize/coordinate authentication across their systems. RADIUS is a very common protocol used to manage access to internal networks, Wi-Fi networks, email

services and VPN services. Originally designed to transport authentication information for remote dial up users, it's evolved to carry a wide variety of standard authentication protocols like EAP or Extensible Authentication Protocol. Clients who want to authenticate to a RADIUS server don't directly interact with it. Instead, when a client wants to access a resource that's protected, the client will present authentication credentials to a NAS or Network Access Server which will relay the credentials to the RADIUS server. The RADIUS server will then verify the credentials using a configured authentication scheme. RADIUS servers can verify user authentication information stored in a flat file or can plug into external sources like SQL databases, LDAP, Kerberos or Active Directory. Once the RADIUS server has evaluated the user authentication request, it replies with one of three messages access reject, access challenge or access accept.

- Internal sites should use encryption for their communication sessions with users to prevent eavesdropping and provide for secure communications. Sites that display the HTTPS designation in the browser URL (as opposed to just HTTP) are secured (that's what the S stands for).
- A Proxy server can be configured to monitor/disallow internal access to/from external sites (inappropriate business-use sites for example)
    - Proxies can be really useful to protect client devices and their traffic. They also provide secure remote access without using a VPN. A standard web proxy can be configured for client devices. This allows web traffic to be proxied through a proxy server that we control. This configuration can be used for logging web requests of client devices. The devices can be used for logs, and traffic analysis, and forensic investigation. The proxy server can be configured to block content that might be malicious, dangerous, or just against company policy.
- A host-based firewall (described in more detail below) can also help maintain internal security, because a network firewall or proxy server may not help protect hosts from threats that are already inside the network.

Remote access solution

- VPNs are also recommended to provide secure access to internal resources for mobile or roaming users. VPNs are commonly used to provide secure remote access, and link two networks securely.
- A Site-to-site VPN can be used to connect to remote sites to each other, users in the offices will be able to access resources as if they are all on one network. Traffic is encrypted between the two.
- Also, a reverse proxy can be configured to allow secure remote access to web-based services without requiring a VPN. By configuring a reverse proxy at the edge of the network, connection requests to services inside the network coming from outside are intercepted by the reverse proxy. They are then forwarded on to the internal service with the reverse proxy acting as a relay. This bridges communications between the remote client outside the network and the internal service.
    - This proxy setup can be secured even more by requiring the use of client TLS certificates, along with username and password authentication. Specific ACLs can also be configured on the reverse proxy to restrict access even more. Lots of popular proxy solutions support a reverse proxy configuration like HAProxy, Nginx, and even the Apache Web Server.

Firewall and basic rules recommendations

- Host Based Firewalls should be used on all laptops and desktops.
- The company should also use a Network firewall for incoming/outgoing traffic.
    - Start with an 'implicit deny' rule, so everything is blocked by default, then allow access to necessary traffic. It is easier and more secure to do it this way – to block everything then whitelist or open the network up for only what you need and allow access to sites that are necessary using ACL lists.
- They can adjust the firewall to disable access to printers from outside the network, for example. This reduces their attack surface.

Wireless security

- They should use WPA2 with 802.1x authentication for their wireless network. The Active Directory/LDAP service recommended previously will provide the back-end authentication infrastructure for implementing 802.1X authentication.
    - This can also can be used for wired connections. Clients/supplicants must authenticate to the network before being able to access it.
- They should also use EAP-TLS for secure authentication procedures.

    - Clients can authenticate with a certificate, username/password, and a OTP as well (for highest levels of security).
    - This will require the use of a RADIUS server and authentication "back end" at a minimum.
- If 802.1X is too complex or “overkill” for them to implement, then WPA2-AES with CCMP is the next best thing in wireless security.
    - If using this method, make sure to utilize a long and complex passphrase not found in the dictionary. Also use an uncommon/unconventional SSID (network name).
    - And, DON'T allow the use of WPS for joining clients to the network.

VLAN configuration recommendations

- Network separation or segmentation is recommended. They can use VLANs for different devices, like printers vs. client devices, and put the printers on a separate network, and then configure routing between the network segments to control traffic.
- Can also use VLANs to isolate or quarantine infected hosts during an intrusion.
- The company should segment their network into four separate VLANs at least:
    - An Engineering VLAN
    - A Sales VLAN
    - An Infrastructure VLAN, and
    - A Guest VLAN.

Laptop security configuration

- They should enable firewalls on the laptops/hosts. A host-based firewall provides protection for mobile devices such as a laptop that could be used in an untrusted, potentially malicious environment like an airport Wi-Fi hotspot. Host-based firewalls are also useful for protecting other hosts from being compromised by corrupt devices on the internal network.
- Consider whether or not to give users administrative rights on their machines. This also can reduce the attack surface and prevent malware installation by preventing unauthorized configuration changes (like turning off the host-based firewall, etc.) or prevent users from installing unapproved/unverified software.
- They should use full disk encryption on laptops. In case they are lost or stolen, data will not be recoverable. This is also a good idea for desktops and servers as well. It prevents data theft and tampering.

Application policy recommendations

- Disable unnecessary default components or features in software/applications – this will help reduce the attack surface. Reducing the complexity of the software/code being used will reduce the attack surface.
- Change any application’s default login account credentials if they exist.
- Run anti-malware or antivirus software. Despite its shortcomings, it still protects against the most common attacks.
- Also consider binary whitelisting software for known trusted/good apps, and blacklist everything else. There is a trade off in convenience with this, and it depends on how much/often users will need to download and run their own apps. Binary whitelisting can also be configured to trust software from certain vendors (for software updates and patches, etc.).
- Deploy and maintain a software patch management system to ensure updates and patches are distributed and applied to servers and clients in the organization. Solutions like Microsoft's SCCM allow administrators to get an overview of what software is installed across their fleet of many systems. This lets a security team analyze what specific software and versions are installed, to better understand the risk of vulnerable software in the fleet. When updates are released and pushed to the fleet, these reporting tools can help make sure that the updates have been applied. SCCM even has the ability to force install updates after a specified deadline has passed.
- Institute a policy where only the latest version of a particular software program is supported or allowed for users. This will make sure that software updates and patches are readily available from the software manufacturer and will help reduce the attack surface.
- Disallow some categories of "risky" software, like file-sharing or piracy-related software, like BitTorrent or Usenet access/software. This will also reduce the attack surface.

- Recommend and support a specific, limited set of software for the users, rather than allowing them to use whatever software they want. This will reduce the attack surface and limit the amount/volume of software that IT needs to support and maintain.
- Also consider a whitelisting policy for browser extensions. Extensions can be another attack vector.

Security and privacy policy recommendations

- Incorporating good password policies into an organization is key to ensuring that employees are securing their accounts with strong password. Use complex passwords that contain lower and upper-case letters, numbers, and special characters. Change passwords on a regular basis. Check for potential password reuse/recycling by users. Have good length requirements, character complexity, and check for dictionary words.
- You must also provide a balance between security and usability - making the password policy too complicated or strict will lead to users cutting corners or compromising security (by writing down passwords if they're too difficult to remember, etc.). So, a balance between security and usability must be struck, in order to be as effective as possible.
- Multifactor authentication for users (some or all) is recommended, depending on the sensitivity of customer information the user may have access to. Two-factor authentication via one-time passcodes (sent via text), or a physical or virtual token which generates a new random passcode (either on a timed schedule or an incremental schedule once a code has been used) will increase their overall password security.
- Users should also have mandatory training on security best practices, to help implement a culture of security in the organization.
- Implement a comprehensive privacy policy: Privacy policies oversee the access and use of sensitive data. They also define what appropriate and authorized use is, and what provisions or restrictions are in place when it comes to how the data is used.
    - They also need a way to enforce these policies. Periodic audits on cases where sensitive data was accessed helps ensure that sensitive data is only accessed by people who are authorized to access it, and that they use it for the right reasons.
    - It's good practice to apply the principle of least privilege here, by not allowing access to this type of data by default. You should require anyone that needs access to first make an access request with a justification for getting the data.
- Data handling policies should cover the details of how different data is classified. What makes some data sensitive as opposed to non-sensitive? What's considered confidential data?
    - Once different data classes are defined, they should create guidelines around how to handle these different types of data. If something is considered sensitive or confidential, you probably have stipulations that this data shouldn't be stored on media that's easily lost or stolen, like USB sticks or portable hard drives.

Intrusion detection or prevention for systems containing customer data

- Traffic monitoring. They should monitor normal traffic, so they can better detect abnormal/attack traffic if or when it happens.
- Log analysis is also important. Server logs, firewall logs, application logs should be regularly monitored and analyzed. Log analysis systems with alerts, searching, filtering should be used (like Splunk, for example).
- They can help prevent flood attacks by using software like Fail2Ban – which is a form of IPS.
- They can help prevent rogue DHCP server attacks by enabling DHCP snooping – which sets trusted DHCP server(s), so requests coming from any non-trusted sources are blocked.
- By enabling Dynamic ARP Inspection, they can prevent attackers from redirecting/monitoring network traffic that is intended for a different/legitimate host.
- They should implement a NIDS - Network Intrusion Detection System - to monitor traffic inside the network (beyond what a firewall can see).
    - They can connect a NIDS host and enable port mirroring for the VLAN to be monitored, so the NIDS can see all the traffic on that VLAN.
- They should also utilize a NIPS - Network Intrusion Prevention System - which can monitor network traffic and shut down suspicious behavior. This must be placed within the topology somewhere that traffic will actually flow through it, rather than the NIDS which only needs to be able to see traffic.
    - A NIPS may need to take action on suspicious traffic, so it must be placed in the topology somewhere that it can do that.